CONTROL OF SPACE

- Introduction
- End State
- Key Objectives
  - Assured Access
  - Surveillance of Space
  - Protection
  - Prevention
  - Negation
- Summary Assessment

"The United States must win and maintain the capability to control space in order to assure the progress and pre-eminence of the free nations. If liberty and freedom are to remain in the world, the United States and its allies must be in position to control space."

General Thomas D. White,
Air Force Chief of Staff, 1955

INTRODUCTION

As space products and services become ever more interwoven with our nation's politics, economics, culture, and security, they become an increasingly lucrative target for potential adversaries. With such growing dependence (Figure 5-1), a future foe could gain an advantage by denying, disrupting, or destroying our ability to access and use space.

As space becomes an area of vital national interest, USCINCSPACE must be prepared to protect and defend it. Control of Space is essential to achieving the force multiplying effect of Information Superiority.

Control of Space is the ability to assure access to space, freedom of operations within the space medium, and an ability to deny others the use of

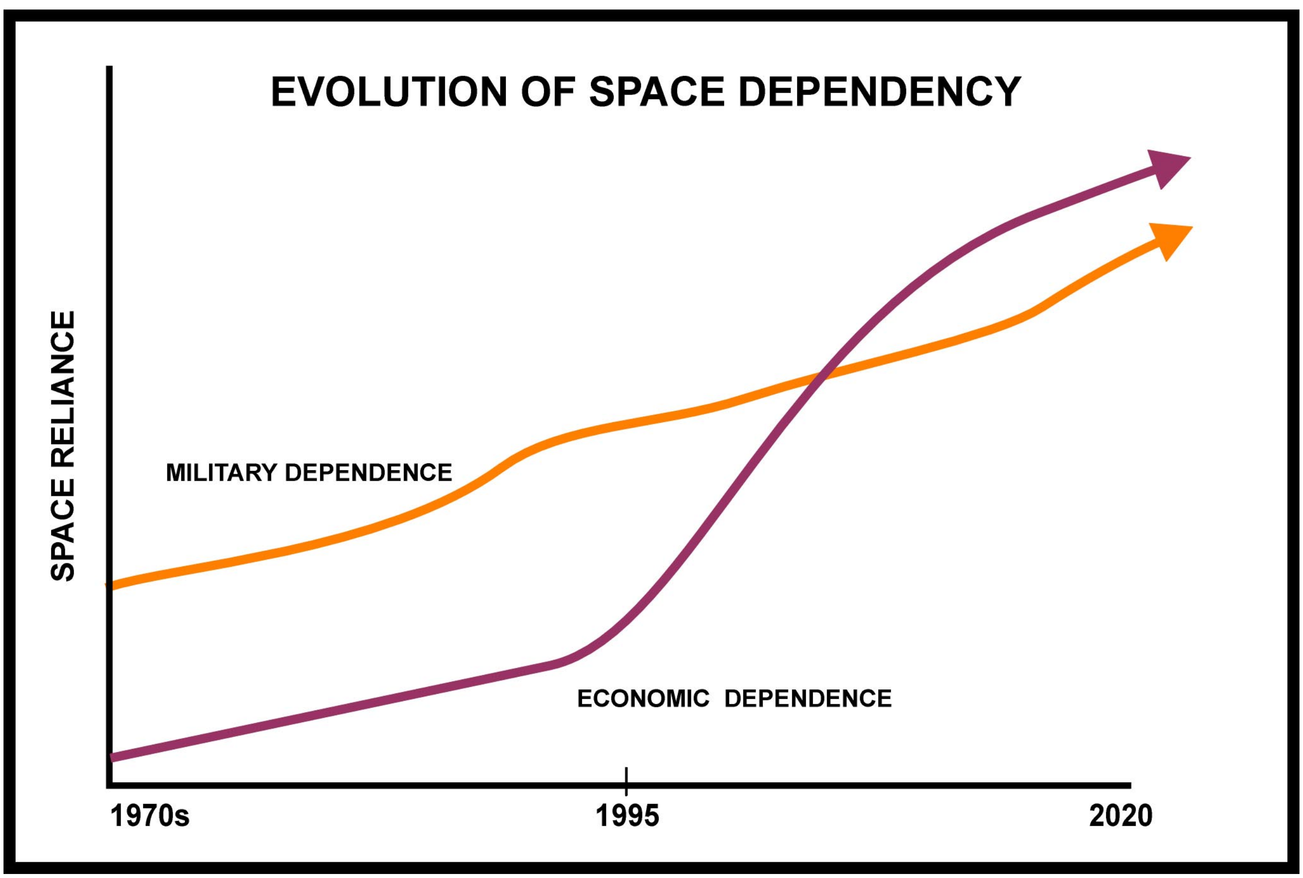


Figure 5-1 Space Becoming a Key to National Interests

space, if required. Achieving and maintaining Control of Space will influence all national and military objectives. Future space programs will be "consumer oriented" to assure information dominance to the warfighter. This operational concept encompasses today's missions of space control and space support (Launch and Satellite Control).

> "Given the importance of space-based capabilities to information operations, our ability to operate in space, support military activities from space and deny adversaries the use of space will be key to our future military success."
>
> *NDP Report, December 1997*

Control of Space requires USCINCSPACE to achieve five interrelated objectives: (1) *assure* the means to get to space and operate once there; (2) *surveil* the region of space to achieve and maintain situational understanding; (3) *protect* our critical space systems from hostile actions; (4) *prevent* unauthorized access to, and exploitation of, US and allied space systems and, when required, (5) *negate* hostile space systems that place US and allied interests at risk (see Figure 5-2).

END STATE

By 2020, we'll have a robust and wholly integrated suite of capabilities in space and on the ground. They will enable us to have situational understanding in space and to ensure access to, through, and from space while defending against all hostile threats. Maintaining dominance of space will require new systems, concepts of operation, and organizations.

The strategy begins with reliable, flexible, and cost-effective means to launch space payloads and

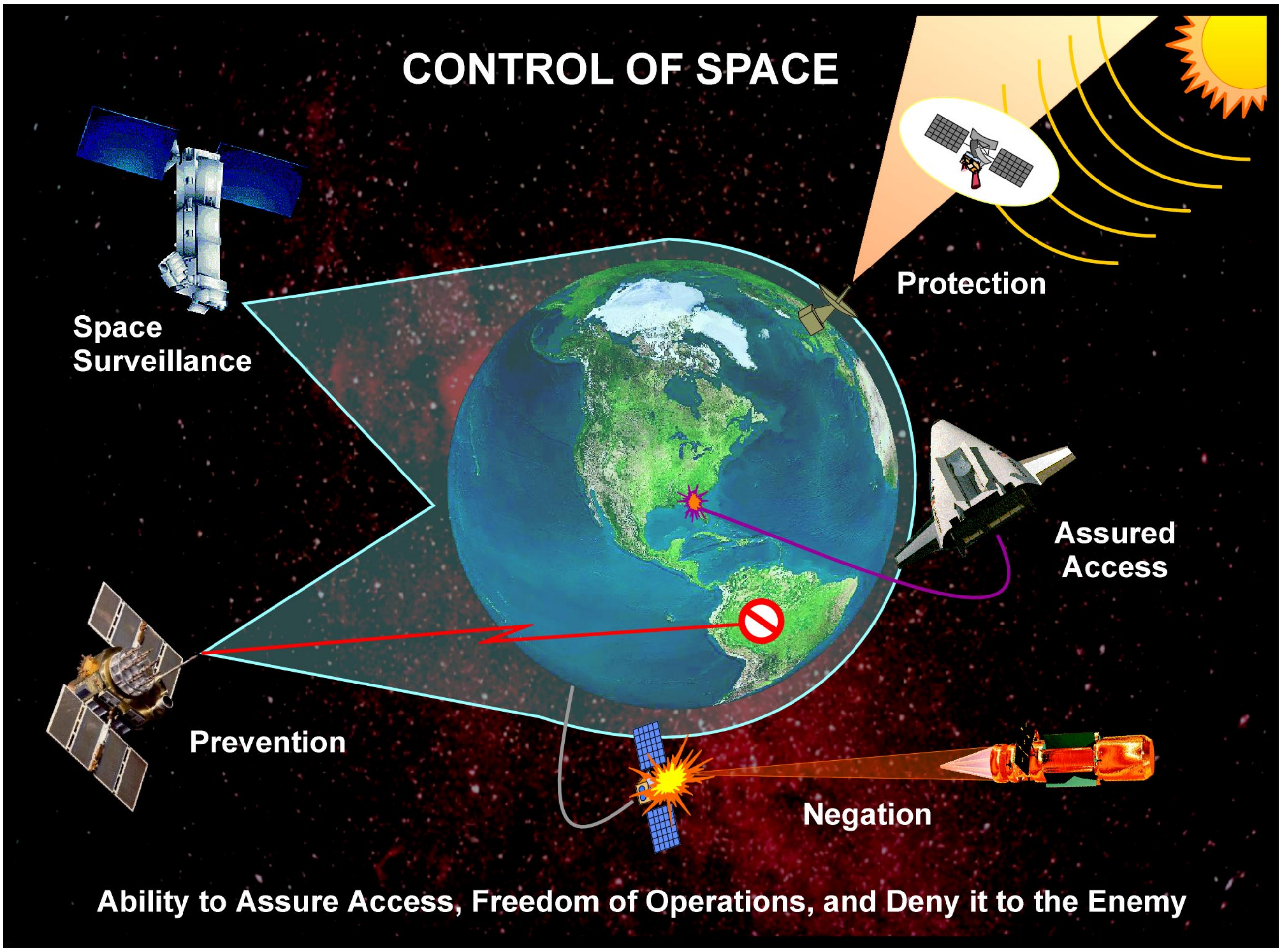


Figure 5-2 Concepts of Operations for Control of Space

operate them once there. Driving the cost of space systems down is important to finding the trade space necessary to provide increased space-based capabilities to the warfighter. *Assured Access* requires a mix of reuseable launch vehicles, expendable launch vehicles, space operations vehicles, and space tugs to deploy, reconstitute, replenish, refurbish, augment, and sustain space systems. The highly dynamic operations tempo in 2020 will require space-based support to be there when needed vice when available. Access to space must be flexible, inexpensive, and available on demand. Command and control of on-orbit assets will be nearly continuous to allow on-demand changes to satellite configurations. National "spaceports" will make access routine, and key partnerships between the DoD, commercial and civil agencies will help manage the increasing space traffic to, through, and from space. Achieving our goals in 2020 will require us to provide timely, low-cost launch and to command and control satellites in near real time.

To assure access to space, we must surveil it. *Surveillance of Space* allows total battlespace awareness, freedom of operations, and deconfliction of activities to, in, and from space–the cornerstones to "enforcing the peace." It also means we must quickly track, identify, characterize, and catalog objects launched into space with ever greater precision. A robust surveillance architecture will spawn a space organization similar to the International Civil Aviation Organization (ICAO)–possibly a much enhanced Space Control Center supported by USSPACECOM Battle Managers. To get there, we'll need a mix of much more capable ground- and space-based sensors, which will provide situational understanding of space in near real time.

With these foundations established, the first priority is to *protect* our vital national space systems, so they'll be available to all warfighters when and where they are needed. Protection requires warning of possible threats (natural and manmade) to US and allied space systems, receiving reports of possible attacks against satellites, cross-cueing other owners or operators, and directing forces to respond to a threat. Space systems must have on-board sensors to detect attacks and quickly report anomalies or suspicious events. The core of protection will be a robust battle manager that receives, processes, correlates, and distributes information reliably, unambiguously, and rapidly. This capability may deter hostile actions against US space systems because, if we know we're under attack, and can quickly identify the source and warn others of the event, an adversary may gain little advantage and choose not to attack.

Prevention denies an adversary's source of power from exploiting US or allied space capabilities, at least temporarily, by any means short of applying military force, including political, informational, or economic. Prevention concepts and systems must be able to identify, report, and distribute audit information on unauthorized access to, and exploiting of, US and allied space systems. USCINCSPACE's main role will be to provide the command, control, and communication architecture necessary to detect and report use and to assess its impact.

Finally, *Negation* means applying military force to affect an adversary's space capability by targeting ground-support sites, ground-to-space links, or spacecraft. Negation will be executed when prevention fails. High-priority targets include an enemy's ability to hold US and allied space systems at risk. Negation will evolve from current concepts, which emphasize terrestrial attacks on an adversary's ground nodes, to a full range of flexible and discriminate techniques against the most appropriate node. Acting under clear lines of authority and rules of engagement, USCINCSPACE will take actions necessary to meet the National Command Authorities' objectives and defend our nation's vital space interests. Actions will range from temporarily disrupting or denying hostile space systems to degrading or destroying them. Our objectives must consider third-party use, plausible deniability and how actions will add to debris or otherwise affect the environment.

A robust battle management capability is crucial to the execution of the entire operations concept. The battle manager will automatically cue systems; fuse information from surface-, air-, and space-based systems; and distribute tailored information from all sources and at multiple levels of security to various users in real or near real time. Besides providing a common operating picture, USSPACECOM Battle Managers will also provide the status of forces, planning tools, decision aids, and execution paths needed to control space. This information will allow USCINCSPACE to select and employ the proper response against threats, assess combat results, and reengage if the threats aren't neutralized. The USSPACECOM Battle Manager will also support a dynamic modeling and simulation capability to support rigorous training, testing, and exercising of joint operations. The USSPACECOM Battle Managers are the key enabler for Control of Space (shown in yellow as CoS in Figure 5-3).

In the following section, this plan addresses the key tasks for each specified objective and the key capabilities needed to achieve the desired end state for 2020. Although we have assigned metrics to each capability, they may change as the plan matures and our vision of 2020 becomes clearer. In other words, the metrics capture the right direction but not necessarily the final destination. For example: for safer human spaceflight, we need to accurately track and avoid smaller objects in space. But the 2020 goal of tracking 1 centimeter objects may change because spacecraft may safely withstand impacts from larger objects.

For each key capability, we also discuss road-maps with associated candidate systems, potential technologies, organizations, CONOPS and partnerships. The systems listed for each specified objective were not necessarily built to meet its requirements for these capabilities. Through the Mission Area Assessment Working Groups, Service components provided candidate systems to achieve the 2020 end state. Finally, we've assessed how well we can achieve these capabilities by 2020.

KEY OBJECTIVES

Assured Access

Assured Access is the "on-demand use" of space lines of communication to enable unimpeded operations in and through space. It's essential to the conduct of space missions (see Figure 5-4). With the dramatic expansion of space operations by 2020, space transport are evolving along lines similar to early aviation–from military, single-use platforms to commercial use. Assured access will involve DoD, national, civil, and commercial organizations, with global partnerships developing to build cost-effective, responsive, flexible systems. Moreover, it is the key to affordable use of space. We must, as a matter of priority, solve the access to space problem in order to free investment to evolve other space capabilities.

Assured Access involves three key tasks:

- *Transporting Mission Assets* to, through, and from space. Encompasses the traditional spacelift mission of delivering payloads to mission orbit and supports emerging missions like negation, missile defense and force application.

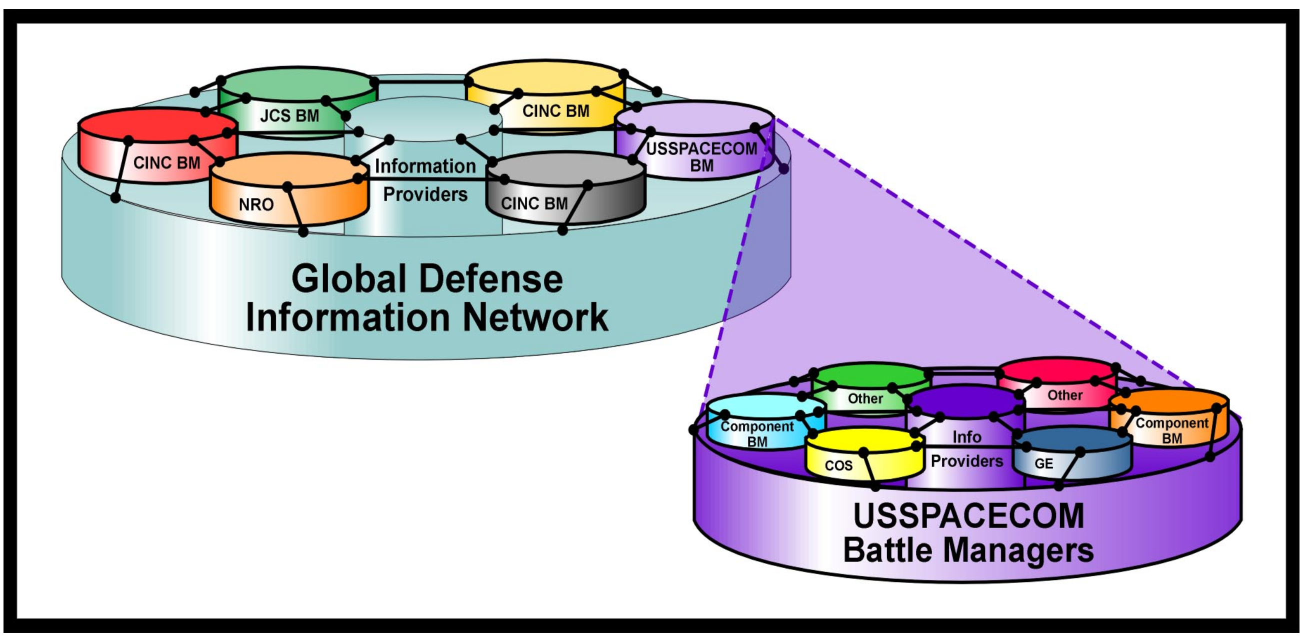
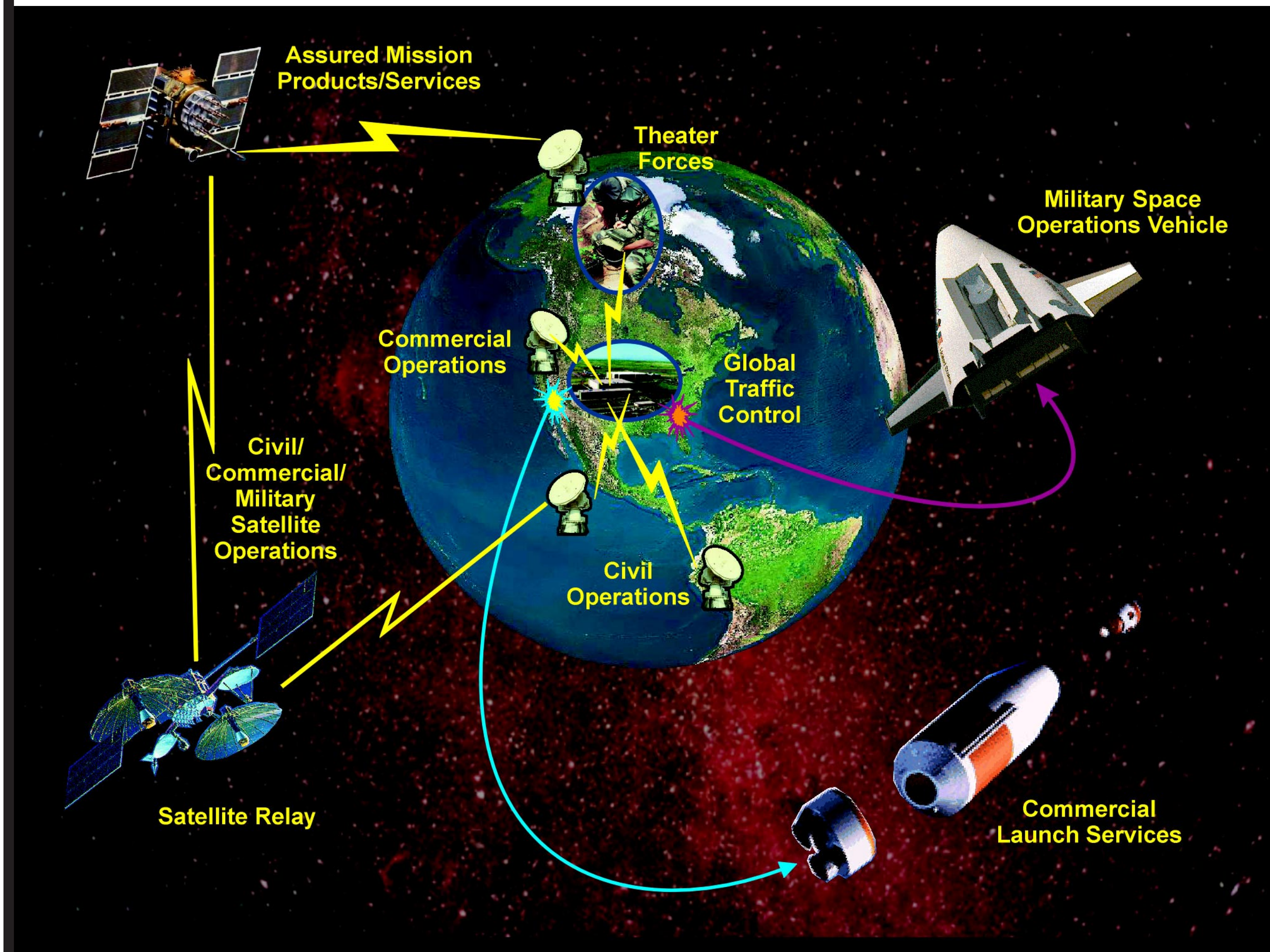


Figure 5-3 Global Defense Information Network and the Battle Managers

ASSURED ACCESS

Provide Freedom of Operations for US/Allied Space Lines of Communication



- *Transport* mission assets to, through and from space; must be routine, inexpensive, responsive and readily accessible.
- *On-Orbit Asset Operations* is integrated worldwide.
- *Service and Recovery* of selected on-orbit assets.

Figure 5-4 Key Tasks for Assured Access

Assured Access transport must be routine, inexpensive, responsive, and readily accessible.

- *Operating On-orbit Assets (Command and Control).* Encompasses traditional satellite-operations missions providing worldwide telemetry, tracking, and commanding (TT&C) for on-orbit satellites. It must be unhampered and uninterruptible and have the ability to analyze status while rapidly retrieving mission data.
- *Servicing and Recovering On-orbit Assets.* Encompasses on-orbit servicing (e.g., replacing black boxes, refueling, and reloading armaments) will be limited to high value systems. Recovery will be available for expensive, low-weight, orbiting sensors and politically sensitive assets that may be deployed for a crisis or war but not needed during peacetime.

Key Capabilities for Assured Access

Based on the three key tasks just described, there are six key capabilities required for 2020. Figure 5-5 depicts the desired warfighting capabilities, current ability, and the goal for 2020.

- *Launch to sustain required constellations for peacetime* operations continues to support the Force Enhancement mission (e.g., navigation, communications, ISR, weather). No dramatic increases are forecast in the DoD's launch rate for this traditional spacelift mission. The goal remains 100% from 1998 to 2020, but we need to sustain forces more efficiently at far lower cost. [Ref: May 1994 Space Launch Modernization Study]
- *On-demand satellite deployment* capability will be necessary starting in 2008, so we can augment and replenish constellations to support crises and combat operations. With the high dependence on space-based systems, launches must be available on demand. [Ref: 1997 DoD/OSA Launch on Demand Impact Study]. Quick replenishment of lost or damaged satellites will lessen vulnerabilities from gaps in coverage. Mission data will be available within days of the identified need for more satellites. On-demand deployment requires all elements (command and control, spacelift systems, satellites, and on-orbit checkout) to react within shortened timelines. The 2020 goal of "within days" derives from anticipating greatly compressed timelines for future conflicts–we'll need to augment satellites before hostilities start to ensure warfighters have enough space-based coverage.
- *Recoverable, rapid-response transport to, through, and from space* will perform negation, force application and missile defense missions. Recallable operations for precision engagement and negation from and through space will need to occur within 2-6 hours of receiving the mission.
- *Global traffic control* will cover the expected dramatic increases in spacelift vehicles transiting to and from space, and the growth of orbital debris. We envision a Federal Aviation Administration (FAA)-like organization to coordinate space operations in near real time, much as an airport does today.
- *On-demand satellite operations execution* will be necessary to manage the expected growth of satellites on-orbit in 2020 [Ref: DoD/OSA Satellite Operations Architecture Study]. To get a single command sequence in today's environment, we have to plan carefully and deconflict resources. On-demand access to any satellite in any constellation, allowing immediate adjustments to orbits and configurations that support time-sensitive military operations is required.
- *Integrated satellite operations mission planning* provides near real time automated planning to enable on-demand execution of satellite operations functions.

Assured Access–Systems Assessment

- *Key Capability–Launch to sustain required constellations for peacetime (100%).* Programmed and planned systems can sustain 100% of the

ASSURED ACCESS	1998	2005	2012	2020
Capabilities				
• Launch to Sustain Required Constellations for Peacetime	100%			100%
• On-Demand Satellite Deployment	Prep - Years/Months Alert - Hours	Prep - Weeks		Prep - Days Alert - Hours
• Recoverable, Rapid Response Transport to, through, from Space	Prep - Months			2-6 Hours
• Global Traffic Control	FAA Pre-departure Collision Avoidance	Prep - Weeks		Integrated NRT Coordination
• Execute Satellite Operations on Demand	Limited Missions	DoD Satellites		All Required Applications
• Integrated SATOPS Mission Planning				
• Responsiveness	Days			Minutes/NRT
• Processing	Manual			Automated

Figure 5-5 Assured Access Capabilities and Goals for 2020

required constellations but not necessarily at an effective cost. This capability will require the use of Atlas, Delta, and Titan launch vehicles for the near term. In 2002, the Evolved Expendable Launch Vehicle (EELV) will reduce launch costs by 25-50% and lift medium-sized payloads within 45 days. EELV heavy lift, with a response time of within 90 days, will come on line in 2003. Commercial services will launch most routine DoD payloads starting in 2006. The Space Operations Vehicle (formerly the Military Spaceplane) should begin to fly around 2012 and may provide another way to routinely sustain constellations. In 2012 or so, new DoD constellations such as Space-Based Radar and Space-Based Lasers will most likely require launchers that handle super-heavy payloads.

- *Key Capability–On-demand satellite deployment (days/hours).* Planned systems have limited potential to meet this requirement, so we'll need new systems for launch on demand. Elements include readily available, quick-reaction, spacelift systems and a full complement of "load-and-launch" satellites designed for streamlined checkout on orbit. Candidates for the spacelift element include commercial expendable launch vehicles (ELVs), commercial reusable launch vehicles (RLVs), advanced upper stages, Space Maneuver Vehicles, and Space Operations Vehicles (SOVs).

- *Key Capability–Recoverable, rapid response transport to, through, and from space (2-6 hours).* Planned, but not programmed, systems may meet this requirement for quick-response, recoverable spacelift vehicles. The SOV in 2012 will be the key platform, but around 2005 space-maneuver vehicles will allow for recovery of sensitive assets in orbit. The SOV's unpredictable launch times and azimuths coupled with tremendous speed ensures commanders retain the advantage of surprise while operating well above current and projected threats.

- *Key Capability–Global traffic control (Integrated NRT).* Planned, but not programmed, systems can meet some of the goals for controlling global traffic. However, a space-based range system is required by 2009 to monitor all vehicles transiting to and from space. This function could consolidate with space surveillance and the FAA's air traffic control systems of the future.

- *Key Capabilities–On-demand satellite operations execution (all applications) and Integrated SATOPS mission planning (automated/NRT).* Planned, but not programmed, systems can meet these goals. Fielding a Space-Based Relay System in 2009 will enable direct access to any satellite, regardless of its position, by cross-linking within a network of relay satellites. This system will also contribute to more efficient and responsive planning to configure resources. In the far term, a virtual satellite-control network will allow dial-in control from a personal computer at any location, thus safeguarding command and control, if key nodes are eliminated.

Assured Access–CONOPS, Organizations, Global Partnerships and Policies

Around 2004, commercial spacelift will largely supplant the DoD's spacelift fleet because it will be so dependable. For DoD to use commercial spacelift, we'll need to resolve the policy issue of launch priorities. The nation will need to build consensus by 2005 on whether reusable launch vehicles make sense and then determine the proper mix. Demand for commercial launches will far exceed that for DoD launches by 2004. Thus, opportunities will arise to partner with industry so we can convert launch ranges to commercially managed spaceports (analogous to airports) that will provide spacelift infrastructure and range control. To do so, we'll need to negotiate agreements with the Department of Transportation and the commercial providers starting around 2001. For "load and launch" CONOPS, spacelift systems and force-enhancement satellites must be readily available with short preparation time. Standard interfaces between launch vehicles and satellites will help select the launch vehicle based on availability and mission profile. The increases in spacelift traffic call for merging the launch ranges' safety control function and air traffic control into an FAA-like space organization. The resulting global traffic control will require collaboration among the DoD, Department of Transportation, FAA, civil, US commercial, and international space-lift communities, and international traffic-control organizations. To ensure access to frequencies needed for commanding satellites, the DoD must coordinate with other government agencies and commercial interests. An integrated satellite operations mission planning CONOPS will optimize on-demand commanding and streamline resource planning.

Figure 5-6 shows the roadmap for Assured Access.

Assured Access–Overall Assessment

The overall assessment for Assured Access is GREEN in 2020 provided the US acquires the required systems, supporting technologies mature, and CONOPS, organizations, and partnership opportunities develop. For the transition period, having launch on-demand by 2008 drives Assured Access from RED to YELLOW. Although the Space Operations Vehicle will arrive by 2012, the assessment won't

Assured Access

Key Capabilities	Candidate Systems 98	05	12 20	Candidate Technologies
Launch to Sustain Required Constellations for Peacetime Operation (100%)	Atlas, Delta, Titan EELV Commercial Launch Services	Advanced Upper Stages Space Maneuver Vehicles	Super Heavylift Space Operations Vehicles	Reduced-cost launchers Advanced Upper Stages (AUS): fuels, propulsion, power, avionics Space Maneuver Vehicles: fuels, propulsion, power, avionics RLVs/SOVs: propulsion, fuels, structures, Thermal Protection System (TPS), operations & maintenance (O&M), power, avionics, manufacturing & processing (M&P)
On-Demand Satellite Deployment (Days/Hours)	Atlas, Delta, Titan EELV Commercial Launch Services	Launch on Demand Systems Advanced Upper Stages Space Maneuver Vehicles	Space Operations Vehicles	LOD: Standard interfaces, M&P, O&M, load & launch' payloads, shortened on-orbit checkout AUS: fuels, propulsion, power, avionics ST: fuels, propulsion, power, avionics RLVs/SOVs: propulsion, fuels, structures, TPS, O&M, power, avionics, M&P
Recoverable, Rapid Response Transport to, through, and from Space (2 - 6 Hours)		Space Maneuver Vehicles	Space Operations Vehicles	Space Maneuver Vehicle: structures, avionics, power, TPS RLVs/SOVs: Propulsion, fuels, structures, TPS, O&M, power, avionics, M&P
Global Traffic Control (Integrated NRT)	Range Standardization & Automation		Space-Based Range	Improved weather forecasting
On-Demand Satellite Ops Execution (All Required)	Current Grd Sys Mobile/Trans-portable Systems ARTS Upgrade	Space-Based Relay	Virtual Satellite Control Network	Advanced antennas Precise on-board navigation Advanced human-computer interfaces
Integrated SATOPS Mission Planning (Min/NRT, Auto)	Automated Scheduling Tools for Range Operations	Space-Based Relay	Virtual Satellite Control Network	Advanced tools for modeling & simulation Advanced processing Advanced/improved application software Standard Adaptive Comm I/F
CONOPS	Commercial Spacelift Spaceports Integrated SAT-OPS Mission Planning Freq. Allocation Decision	Load & Launch Standard Interfaces Space FAA/ICAO		
Organizations	Spaceports	Space FAA/ICAO Space Force TC	Global Traffic Control	
Global Partnerships and Policies	Launch Priorities ELV/RLV Mix Decision Spaceport Transition Freq. Allocation Decision	Space FAA/ICAO	Global Traffic Control	

Figure 5-6 Assured Access Roadmap

move from YELLOW to GREEN until these vehicles are acquired and in sufficient number by 2018. Satellite operations are a strong YELLOW because of the virtual satellite-control network which will allow operator access through desktop computers. Figure 5-7 shows this assessment.

Assured Access–Technology Assessment

New launch-processing techniques are needed to reduce timelines and costs that currently prohibit launch on demand. Reusable vehicles–such as the Space Operations Vehicle or NASA's technology demonstrator, X-33–may be the solution. If so,

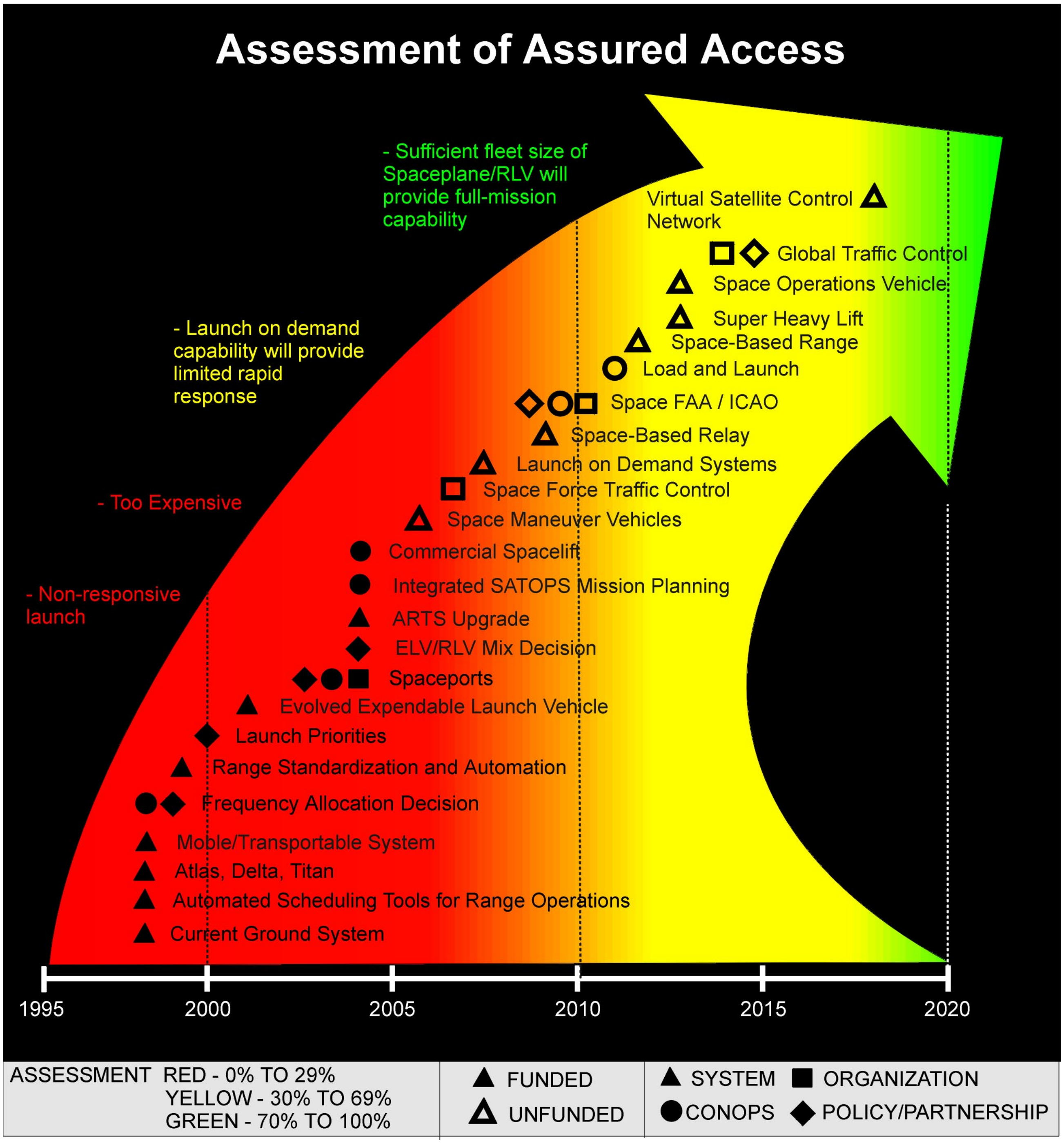


Figure 5-7 Assessment of Assured Access

they'll require lightweight, durable materials for thermal protection and improvements in propulsion system operability and reusability. They will also need advanced launch-processing techniques, such as systems to handle propellants and cryogenic materials, plus new procedures for weather forecasting, integrating vehicles, and payloads and managing ranges. Lastly, expendable and reusable vehicles will need new technologies for tankage, structures, rocket-engine parts, propellant handling, advanced upper stages, and extending the lifetimes of satellite components. Assured Access to space has many dimensions and requires changes in architectures and philosophies, as well as several breakthroughs in technology.

Assured Access–Recommendations and Directives

(**Recommendation**) Determine the future architecture and organization for controlling space traffic.

- Possibly convert military operated launch ranges to national commercially operated spaceports. (AFSPC)
- Revise flight-safety zones for reusable launch vehicles. (AFSPC)
- Establish controls and protections for satellites in low earth orbit. (AFSPC)

(**Recommendation**) Update national policy to protect the DoD's need for space-based frequencies. (SPJ6)

(**Recommendation**) Jointly develop a national technology roadmap that further reduces costs for spacelift. (AFSPC/Labs/Industry)

(**Recommendation**) Fund demonstrations of space-maneuver vehicles for Fiscal Years 2002 and 2003. These vehicles are the key to recovering politically sensitive platforms from space. They also can dramatically change how we use our satellite constellations. (AFSPC)

(**Recommendation**) Revise national policy on launch priorities to benefit all users while accounting for the DoD's transition to commercial launches and the expected emergence of launch on demand. (AFSPC)

Surveillance of Space

Near real-time space situational awareness, enabled by Surveillance of Space is the key contributor to the Control of Space and enabling freedom of operations within it. Future space surveillance capabilities will be the foundation for space superiority. Figure 5-8 depicts the Surveillance of Space key tasks.

Key Capabilities for Surveillance of Space

Based on these key tasks, there are four key capabilities required for 2020:

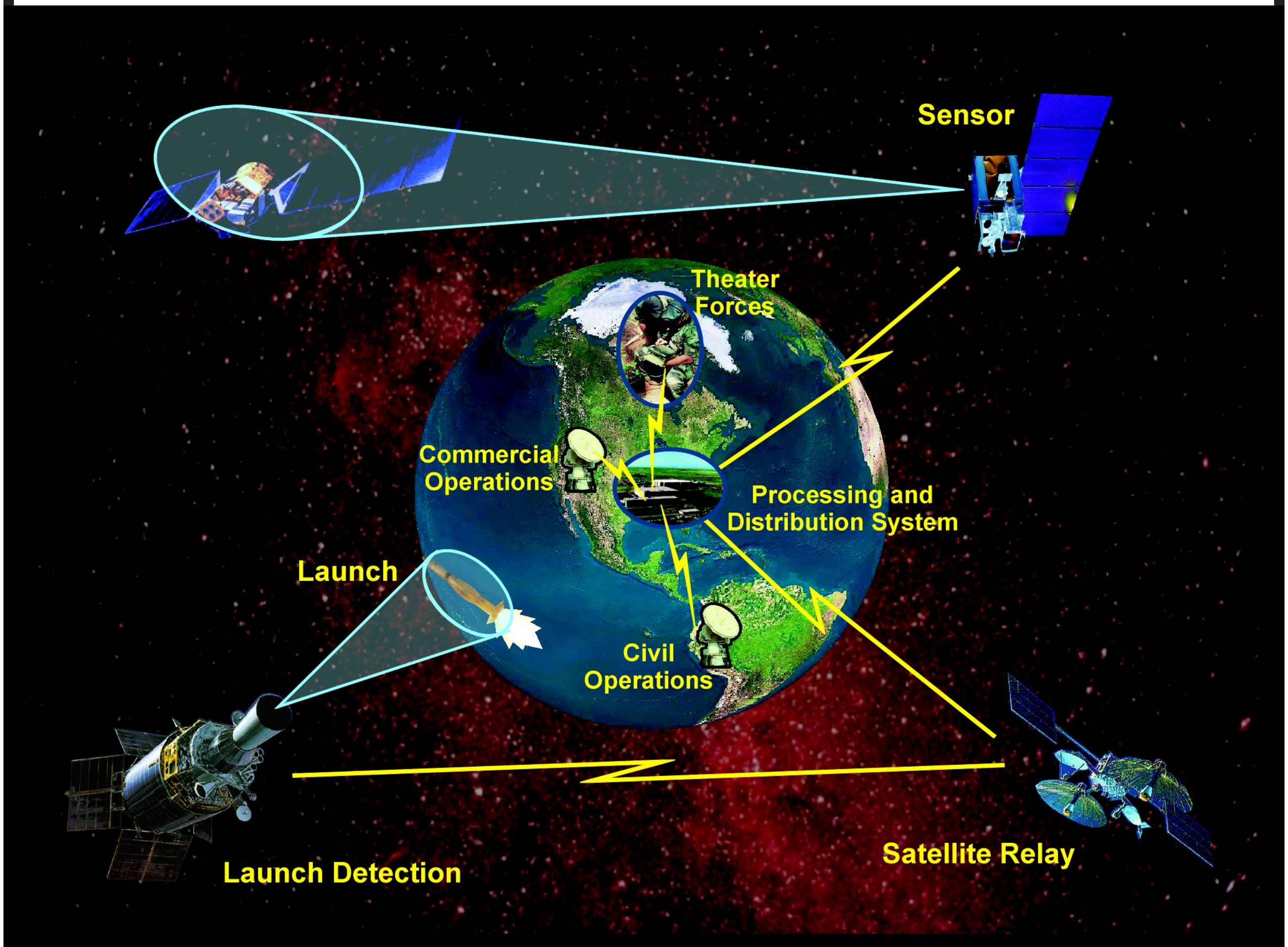
- *Real-time characterization*, soon after launch, for high-interest objects (HIOs) that may threaten US and allied forces (e.g., spaceborne payloads for ISR or antisatellite weapons). This requires sensors that can provide high-quality imagery and electronic intelligence to confirm mission, size, shape, and orientation. Combined with orbital parameters, this capability will classify threats. Real-time characterization is critical because, within two revolutions, payloads can begin collecting information on our forces. Antisatellite weapons could also be deployed within one or two revolutions after launch.

- Precision *detection and tracking* are needed to ensure crewed spacecraft can maneuver freely, to deconflict orbits, and to employ weapons. This ability leads to accurate observational data from multi-mission systems on the ground and in space. Tracking data must be more accurate and abundant than what today's ground systems provide in order to support cataloging and monitoring.

- *Timely surveillance of high interest objects* includes such threats as maneuvers, foreign ISR, and configuration changes to space-based weapons. Solutions will probably have to be space-based because, once a satellite is characterized as a possible threat, timely surveillance becomes critical.

SURVEILLANCE OF SPACE

Provide Real Time Position and Characterization of Orbiting Objects



- *Detect*–every launch and all objects
- *Track*–All satellites (all sizes) over entire orbit, for entire orbit lifetime
- *Characterize*–Every launch, payload, owner, mission, capabilities, size, shape, orientation
- *Classify*–Threat
- *Catalog/Monitor*–Characterization data, orbital parameters for all satellites
- *Disseminate/Distribute*–Products and data

Figure 5-8 Key Tasks for Surveillance of Space

- The fourth capability moves from collecting data to cataloging and distributing it. *Space catalogs* are shared with all nations, and with organizations that own or operate space systems. We must have more accurate techniques for numerical integration so we can accurately predict miss distances between orbits for manned missions, such as the International Space Station, the Shuttle, and the Space Operations Vehicle.

Figure 5-9 depicts desired warfighting capabilities, current abilities, and goals for 2020.

Figure 5-10 is the roadmap for Surveillance of Space.

Surveillance of Space-System Assessment

- *Key Capability–Real-time Characterization of HIOs (100%).* Programmed and planned systems cover part of the need, but sensors aren't distributed enough, imaging is marginal, and characterization isn't timely. The single Forward-Based X-Band (FBXB) Radar is specified as a sensor for national missile defense and, therefore, will not conduct space surveillance as a primary mission. The conceptual Space-Based Electro-Optical Network (SBEON) and Radar Imaging & Deep Space Network (RIDSN) add only a little to our characterizing needs. Existing or planned sensor technologies can increase accuracy, but processing and "packaging" of data must improve to achieve the desired end state.

- *Key Capability–Detect/Track Satellites Over Entire Orbit (size: LEO 1cm, GEO 10cm; location: LEO 10m, GEO 100m).* Programmed and planned systems can meet some of this need. Existing systems are sparse in orbital coverage, insufficiently spread to meet coverage requirements, and their data isn't accurate enough. Have Stare is not particularly well suited for detecting and tracking near-earth satellites but will provide high-quality data on some high-interest objects. The S-Band Fence upgrade will detect smaller objects. Developing a high-quality space catalog will depend greatly on the planned SBEON's performance. SBIRS Low should cover whole orbits but not accurately enough.

- *Key Capability–Timely Surveillance of High Interest HIOs–(NRT).* Programmed and planned systems do little to achieve this capability. The S-Band Fence upgrade will allow us to detect smaller objects but won't detect maneuvers in near real time. More sensors will cover each orbit for all high-interest objects but may not be accurate enough. The planned SBEON and RIDSN will work better for time-sensitive operations. SBIRS Low should contribute to surveillance of objects in near real time.

- *Key Capability–Space Catalog/Monitoring–(NRT).* Highly accurate data on all satellites are needed to keep clearances between them, locate reentries, and track orbits of newly launched space vehicles. Existing and planned systems begin to deliver these capabilities. The number of sensors, data accuracy, and computational capacity must increase to more precisely determine and predict orbits for the 2020 catalog. Again, the S-Band Fence upgrade will allow us to detect smaller objects. If observational data from SBEON or RIDSN is highly accurate, it will help us maintain the catalog and monitor objects. The Transportable Optical System (TOS) is a single telescope designed only for GEO. If its accuracy is similar to that of the GEODSS, it will help us maintain and monitor

SURVEILLANCE OF SPACE	1998	2005	2012	2020
Capabilities				
• Real-Time Characterization of High Interest Objects	0%	50%		100%
• Detect/Track with Precise: Size LEO/GEO; Location LEO/GEO	30cm/30cm 1km/5km	10cm/20cm 500cm/2km		1cm/10cm 10m/100m
• Timely Surveillance of High Interest Objects	Days/Hours			NRT
• Catalog/Monitoring	Predictive			NRT

Figure 5-9 Surveillance of Space Capabilities and Goals for 2020

Surveillance of Space				
Key Capabilities	Candidate Systems			Candidate Technologies
	98	05	12 — 20	
Real Time Characterization of all HIOs (100%)	FBXB Radar	SBEON RIDSN CoS BM	USSPACECOM BM	Spectral, SAR, ATR Processing, Cross-Cueing
Detect/Track With Precise: Size & Location (LEO/GEO) (Size 1cm/10cm, Location 10m/100m)	HAVE STARE FBXB Radar	SBEON S-Band Fence SBIRS-Low		Spectral, SAR, MTI
Timely Surveillance of HIOs (NRT)		SBEON S-Band Fence RIDSN SBIRS-Low		MSX, Cross-Cueing
Catalog/ Monitoring (NRT)	TOS	SBEON S-Band Fence RIDSN	GDIN	Fusion Processing
CONOPS	CMAS/Component C2 Centers USSPACECOM BM	International Ops Centers		
Organizations		International Surveillance Net	USSPACECOM BM	
Global Partnerships and Policies	Satellite Self ID and Reporting Policy		Satellite Inspection Policy	

Figure 5-10 Surveillance of Space Roadmap

today's catalog but won't help meet the requirements of 2020. Angular data will have to be far more accurate. SBIRS-Low is designed as a missile-warning asset, so it probably won't be able to provide the accurate observations needed to maintain the catalog in 2020.

Surveillance of Space–CONOPS, Organizations, Global Partnerships and Policies

The future CONOPS for surveillance systems will likely remain with the DoD, NASA, and related agencies such as the labs, or even the Russian Space Agency. We can also integrate some allied or foreign surveillance capabilities into an international operations center. However, centralized surveillance of space by USSPACECOM remains critical to optimal mission performance, standardization, responsiveness, and data integrity. Various distributed processing architectures will fuse data from all sources into the required space products and rapidly distribute them to forward users. These users will access the centralized database for space surveillance to get what they need. In 2020, several new or different organizations including an international space-surveillance net, may catalog space objects. USSPACECOM, AFSPACE (14 AF), and Naval Space Command will combine resources with allied, civil and industry partners–such as NASA, Canada, the European Space Agency, and the Russian Space Agency–to establish and maintain a space catalog.

NASA, Canada, the European Space Agency, and the Russian Space Agency are prime candidates for forming partnerships to perform satellite self-identification and reporting. In addition, pre-launch inspections could ease the burden of characterizing satellites. Finally, an international policy on space debris could slow the growing number of objects that require tracking and cataloging.

Surveillance of Space–Overall Assessment

The overall assessment for Surveillance of Space is YELLOW because all key capabilities have shortfalls. More sensors of higher quality, better orbit coverage and better observational data are needed to locate objects more precisely. We'll need improved or new technology to characterize objects more accurately in real time. Figure 5-11 shows this assessment.

Surveillance of Space–Technology Assessment

Migrating space surveillance from the ground to space will require some technological advancements.

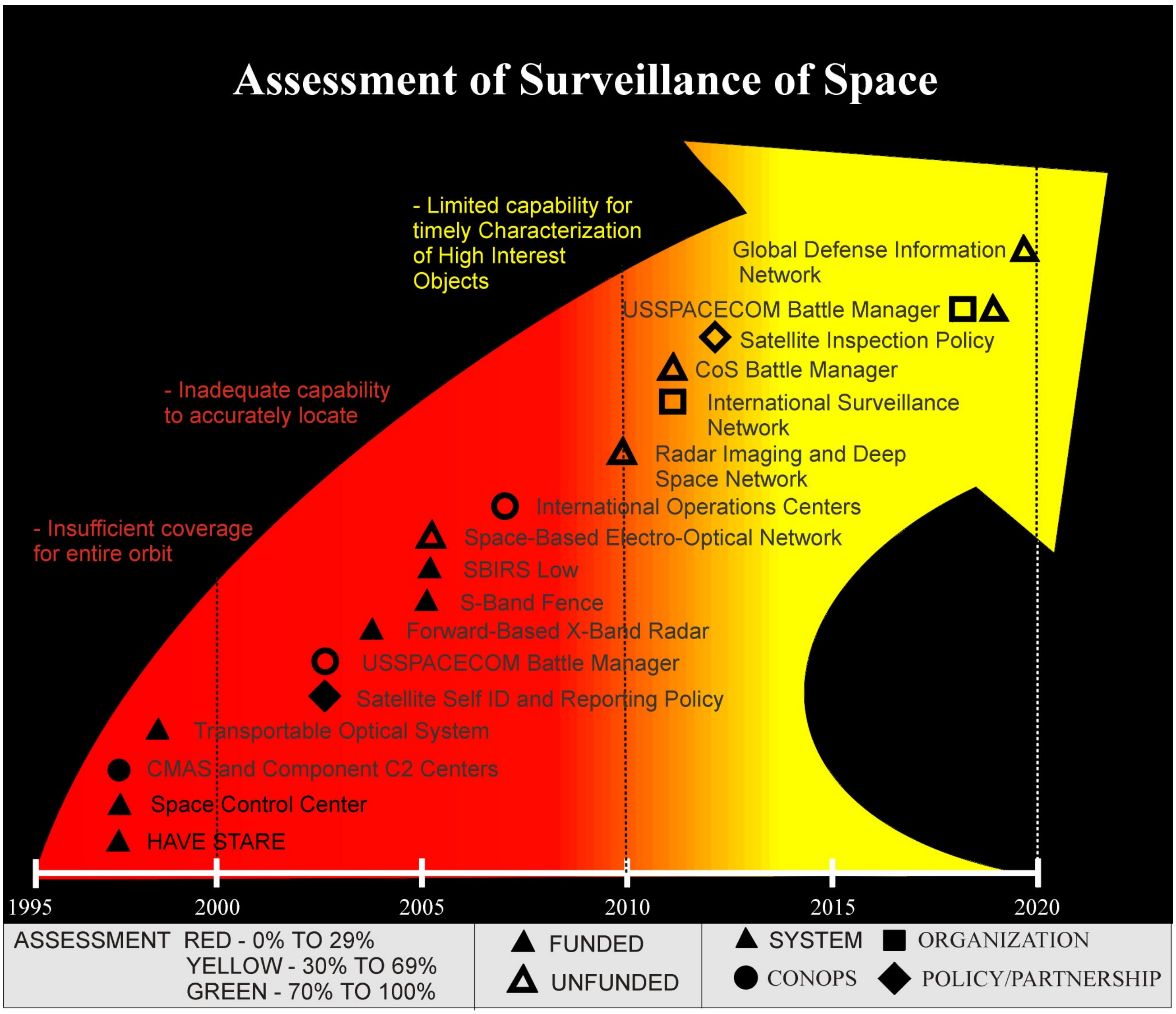


Figure 5-11 Assessment for Surveillance of Space

Many of the technologies supporting space-based surveillance are similar to those supporting Global Engagement's requirements for Integrated Focused Surveillance. This includes technology development for passive (e.g., electro-optical, bistatic, infrared) and active (e.g., radar, LIDAR/LADAR) sensors. As with other surveillance systems, a very good understanding of target signatures and backgrounds is critical to any surveillance system's success. Additionally, the data processing, algorithms, and data fusion for space surveillance is equally important to meet cataloging requirements. This may require onboard software for processing, hardware developments, and advancements in intelligent expert systems.

Space-based surveillance places a heavy requirement on developments in spacecraft-positioning systems; guidance, navigation, and control techniques; cryocoolers; batteries; structures; highly-efficient solar arrays; and vibration suppression. Additionally, satellite crosslinks will be required for cross-cueing, target tip-off, and highly accurate search and detection.

Finally, the ground segment (including command and control and data processing) also requires upgrades that have their own technical challenges. Some of the technologies required for robust command and control include handling information, processing data, developing algorithms, fusing data, intelligent systems, and human-machine interfaces.

Surveillance of Space–Recommendations and Directives

(**Directive**) Develop modeling and simulation to analyze the performance of proposed systems and sensors. These analysis tools will be instrumental to studies, analyses, trades, and future operational concepts for space surveillance. (N-SP/AN)

(**Recommendation**) Examine new and enhanced sensor technology. (Labs)

(**Recommendation**) Review and update space surveillance policy on distributing data; including all military and national systems, as well as envisioned partnership systems. (SPJ5)

Protection

Protecting the US interests in space is critical to our economic, informational, and military welfare. Although the notion of space as a sanctuary appears seductive to many, our increasing reliance on space systems, and information derived from space, creates a *center of gravity* potential adversaries clearly understand. From a military perspective, Protection takes on a new dimension as non-DoD systems (commercial and third-party) become even more integrated into plans for using joint forces. Protection includes active and passive defensive measures to minimize threats (natural and man-made) to space systems, (space, links, and ground segments) as shown in Figure 5-12.

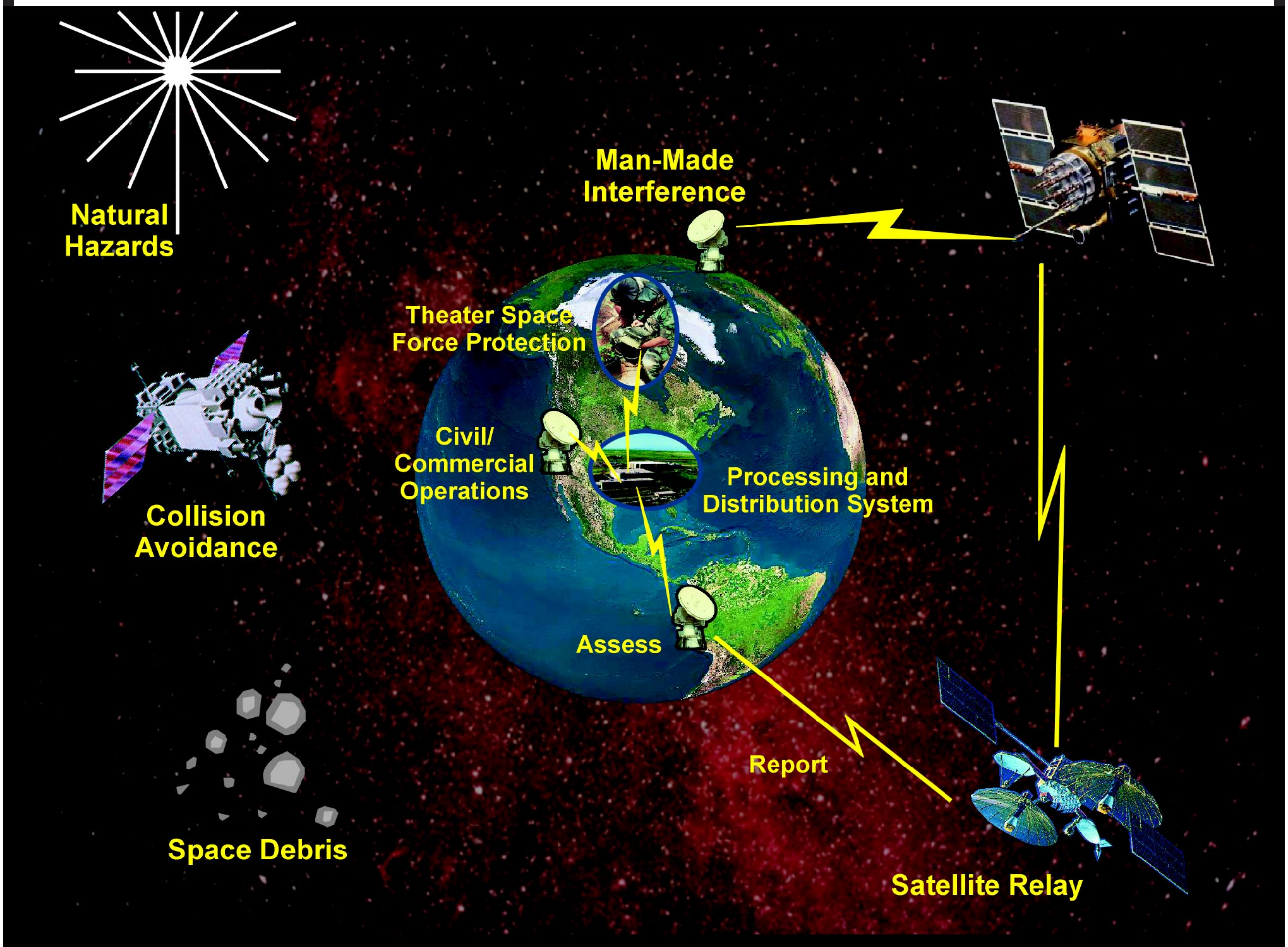
Key Capabilities for Protection

Based on the key tasks in Figure 5-12, Protection requires five key capabilities for 2020:

- *Detecting and reporting threats or attacks* against all space systems of national interest in near real time is critical. Our growing reliance on space systems and services mandates this ability. For current space systems, we determine spacecraft anomalies by analyzing them after they occur. Characterizing anomalies onboard in near real time would permit operators to correct them quickly.
- The ability to *withstand and defend* against attacks on space systems preserves key operational capabilities. Prompted by this rise of counterspace systems, rigorous protection of space systems is essential. Increasing use of civil or commercial space systems will likely require as much attention for these systems as is traditional for national security systems.
- *Reconstituting and repairing* space capabilities critical to national interests (if defenses fail) must occur within days, or even hours. Systems must allow rapid recovery from the temporary effects of jamming, spoofing, or blinding. This includes options for launch on demand, quickly rerouting or retasking capabilities to other systems, and internal redundancies. Each Force Enhancement mission area should develop CONOPS and requirements to achieve this capability.

PROTECTION

Detect, Report and Protect Against Natural and Man-Made Interference/Threats/Hostile Attacks



- *Detect and Report Threats/Attacks*–All threats and attacks to key US/Allied space systems
- *Withstand and Defend*–Key systems from attack, through selective hardening, maneuvering or countering
- *Reconstitute and Repair*–Loss of vital space capabilities in days/hours
- *Assess Mission Impact*–Of space capabilities and disseminate information in seconds
- *Identify, Locate and Classify*–Source of threats or attacks

Figure 5-12 Key Tasks for Protection

- *Assessing mission impact* is critical to course of action development. Current satellite system anomalies caused by external forces require hours to weeks to process. In 2020, the significance of potential or actual hostile actions must be accurately assessed within seconds to allow proper responses or to find other ways to distribute information that satellites produce. Also, if owners and operators are to protect their systems, they must get information on threats and attacks almost immediately.
- *Identifying, locating, and classifying* the source of a threat, ranging from intentional hostile acts to accidents or naturally occurring space events pose great challenges. Quickly and accurately characterizing and correlating what may otherwise appear to be unrelated events will become more important as reliance on space systems increases. We'll need a robust battle-management system, plus advanced modeling and simulation capabilities, to achieve the desired end state.

Figure 5-13 depicts the desired warfighting capabilities for Protection, the current ability, and the goal for 2020.

Figure 5-14 is the Protection roadmap.

Protection–Systems Assessment

- *Key Capability–Detect & Report Threats to owner/ operators in NRT (all National Interests).* Programmed and planned systems do not meet goals for detection and reporting. We need a subsystem for threat warning and assessment reporting, which would allow comprehensive reporting on status changes. Such systems have been in development for years but haven't become operational because of size and weight restrictions, as well as too many false alarms. Unfortunately today's systems–ill positioned for detecting and reporting threats–will be serving us well into the next century. Today's solution will not provide the desired abilities until the next generation of upgraded systems are launched. On-orbit assets are difficult to retro-fit; as solutions become available it will take a generation of space systems to remedy this situation. The NORAD/USSPACECOM Warfighting Support System (N/UWSS) could provide some connectivity for reporting, assessing, and informing operators about threats.

- *Key Capability–Withstand and Defend against Threats (100%).* Few programs address this capability, but onboard protection systems are developing that will enable space systems to protect themselves until operators can isolate and correct a problem. These systems should be ready by 2012.

- *Key Capability–Reconstitute and Repair space services (hours/days).* Programmed and planned systems do little to achieve this capability. Mobile mission processors provide limited redundancy. Space-based relay systems, under development, will protect links and reduce dependence on vulnerable overseas ground sites.

- *Key Capability–Assess Mission Impact/ Disseminate (seconds).* We have no programmed or planned systems. Space-based relay systems will help warn owners and operators, but no automated systems provide an assessment. Advanced modeling and simulation capabilities can help here.

- *Key Capability–Identify/Locate/Classify source with high confidence (seconds).* Programmed and planned systems will do this to some extent, but the subsystem for warning and assessment reporting mentioned earlier may greatly enhance protection of space assets. Characterizing missions can also help by giving advanced knowledge of possible threat sources.

PROTECTION	1998	2005	2012	2020
Capabilities				
• Detect and Report the Threat or Attack	0%	Military Significant		National Interests
• Withstand and Defend	10%	50%		100%
• Reconstitute/Repair	Months/Years	Days/Months		Days/ Hours
• Assess Mission Impact/ Disseminate	Hours	Minutes		Seconds
• ID/Locate/Classify Source	Weeks	Seconds		Seconds

Figure 5-13 Protection Capabilities and Goals for 2020

Protection					
Key Capabilities	**Candidate Systems** 98	05	12	20	**Candidate Technologies**
Detect/Report Threats (National Interests)		TW/AR N/UWSS			Artificial Intelligence See Surveillance of Space
Withstand and Defend (100%)			On-board Protection Suites		Radiation Hardening and Shielding, On-board Maneuvering
Reconstitute and Repair (Hours/Days)	Mobile Mission Processors	Space-Based Relay			On-board Diagnostics, Cross-cueing
Assess Mission Impact/ Disseminate (Seconds)	N/UWSS	Space-Based Relay CoS BM	GDIN USSPACECOM BM		Artificial Intelligence, On-board Diagnostics
ID/Locate/ Classify Source (Seconds)	N/UWSS	TW/AR RIDSN	Space-Based Radar		On-board Processing See Surveillance of Space
CONOPS	Post-event analysis, USSPACECOM BM		Adaptive/ Predictive		
Organizations	JFSCC-Like	Space Force Traffic Control	Global Traffic Ctrl USSPACE BM		
Global Partnerships and Policies	Space Law International Protection Agreements				

Figure 5-14 Protection Roadmap

Protection–CONOPS, Organizations, Global Partnerships and Policies

Today, Protection operations depend on post event analysis because systems can't detect and identify sources in near real time. By 2020, the United States must have protection systems and CONOPS that can detect an event and predict its effect on mission operations. Defensive operations, in near real time, require a robust battle manager to provide situational awareness.

The same organizational changes proposed for Space Surveillance and Assured Access will contribute significantly to this objective. In addition, laser-clearinghouse and collision-avoidance programs, out of the Cheyenne Mountain Operations Center, will prevent inadvertent illumination and ensure collision avoidance for high-value payloads. They will expand to assume a role in traffic control for space forces. In addition, a Joint Space Force Component Commander-like position will help determine how to protect forces. We don't intend to prescribe how a regional CINC should organize their space forces; we're merely stating the need to organize for space. Eventually an organization could emerge to handle global traffic control as the FAA and ICAO do now for air travel.

Our increasing reliance on civil, commercial, and international space systems makes partnerships, laws, and agreements to protect these assets a key to preserving them. To do so, we must jointly develop onboard protection for all parties. As the DoD secures more space services from commercial sources, they'll need agreements that require the sources to protect their assets, so systems will be available through all levels of conflict. The combination of growing manufactured threats (orbital debris and antisatellite systems); the harsh space environment (Solar Max in 2007); and the need to ensure space services are available to a demanding consumer, will lead industry to incorporate some measures of protection on their own. Any future treaties must be carefully worded to ensure we can protect space systems of national interest while still denying an adversary the hostile use of space.

Protection–Overall Assessment

The overall assessment for PROTECTION in 2020 is low YELLOW because all capabilities have shortfalls (see Figure 5-15).

Protection–Technology Assessment

Achieving a GREEN rating depends on very immature technology, which requires immediate attention. Although many of the technologies (related to the information stream) are similar to those for Prevention, some threats will require unique technology. For example, the emergence of energy weapons demand entirely new technologies, such as shielding, onboard maneuvering, and

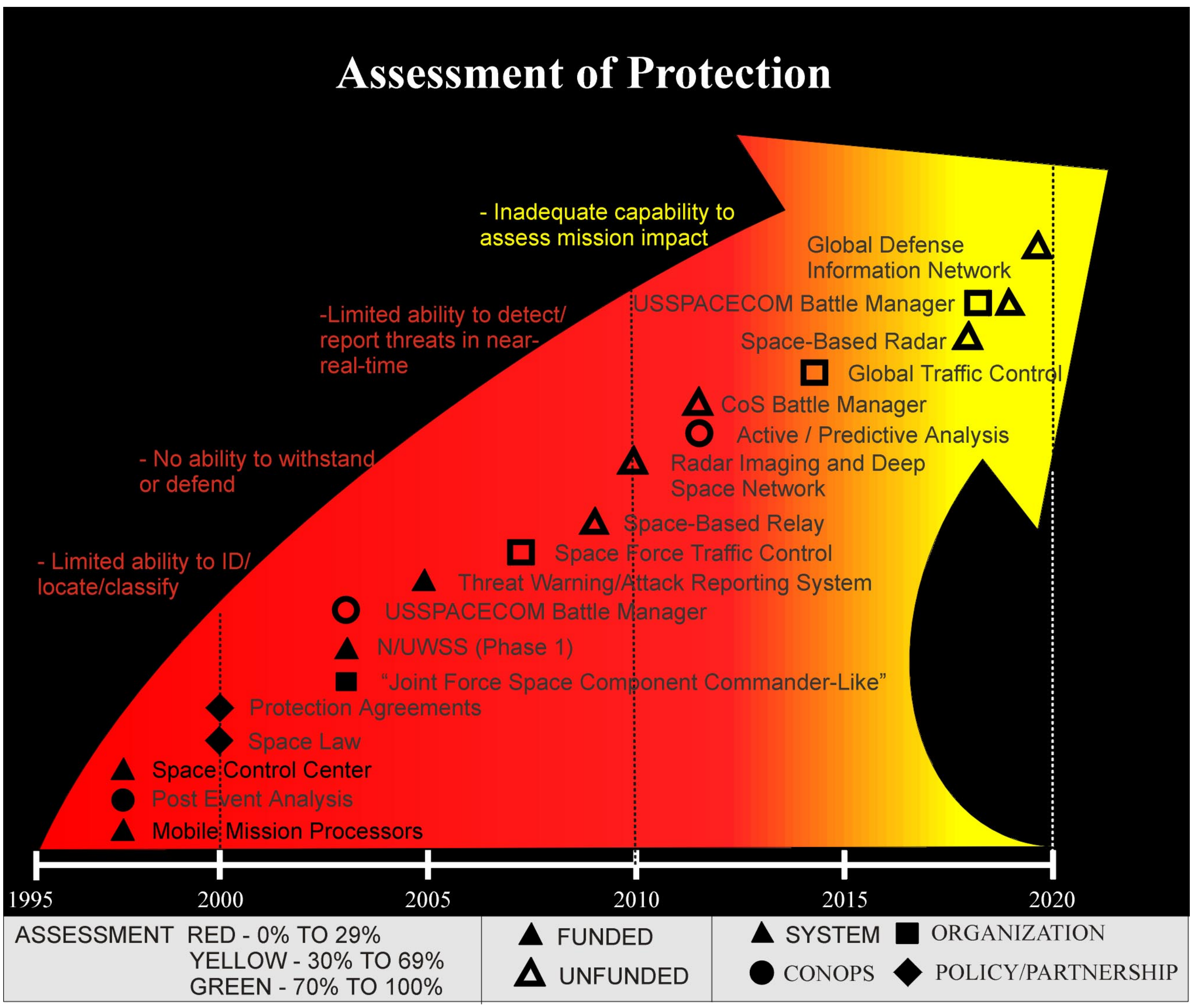


Figure 5-15 Assessment of Protection

hardening, for satellites to protect themselves. Advancement in artificial intelligence, on-board processing, miniature packages and attack sensors will contribute a lot to Protection. Technologies discussed under Surveillance of Space may satisfy some requirements for identifying, locating, and classifying objects in space. These are but a few of the technology challenges we must overcome to protect satellites. We're also looking forward to the results of the threat warning and assessment reporting demonstration (scheduled for 2000).

Technology requirements for satellite communications and control will affect satellite protection. They include exception reporting, onboard diagnostics and repair, and satellites that can work on their own.

Protection–Recommendations and Directives

(**Directive/Recommendation**) Pursue an automated capability to detect, identify, and report in near real time on threats or attacks to US and allied space systems (SPJ3/Labs).

(**Directive/Recommendation**) Pursue policy and possible alliances of space-system owners and operators to process anomalies and analyze trends. (SPJ5).

(**Directive**) Develop advanced models and simulation capabilities to help analyze nodes, identify effects and determine which capabilities we must rapidly reconstitute. (N-SP/AN).

Prevention

Today's concept of Prevention relies on diplomacy and non-military actions to deny an adversary the benefit of space. Prevention links closely to Negation, a concept that applies military force against an aggressor's space systems. Traditionally, these operational concepts have been separate, but commercial uses of space, emerging technologies, and the increased importance of space to the United States and its allies will drive the consolidation of these concepts. Consortia-owned space capabilities will be widely available, and partners, competitors, and rivals will use the same space systems, blurring the traditional distinction among friendly, hostile, and commercial systems. Emerging space and telecommunications technologies will continue to integrate space constellations with other nodes of the infrastructure for global information. As international, civil, governmental, and military systems mingle, we'll need to rely heavily on diplomacy to deny an adversary, but we'll use military actions when vital national interests are challenged and other options can't meet the challenge. In 2020, Prevention will include diplomatic, informational, economic, and military options to preserve freedom of action in space and check an adversary's power. As a result, nations will have to seek consensus on using space. The United States will lead other nations in developing this consensus and will seek coalition support for actions that limit or deny an adversary's use of space.

To understand how Prevention and Negation might combine, let's look at each separately, beginning with Prevention (see Figure 5-16).

Key Capabilities for Prevention

Based on the key tasks listed in Figure 5-16, Prevention in 2020 requires three key capabilities:

- *Detecting unauthorized use* or exploitation of all US or third-party space systems. Widely available space products and services are sophisticated enough to erode the US military advantage and threaten national interests.
- *Assessing the mission impact* with high confidence in near real time. Assessment is necessary for course of action development.
- *Timely and flexible denial* in near real time to curtail an adversary's advantage.

Figure 5-17 depicts desired warfighting capabilities, current abilities, and the goal for 2020.

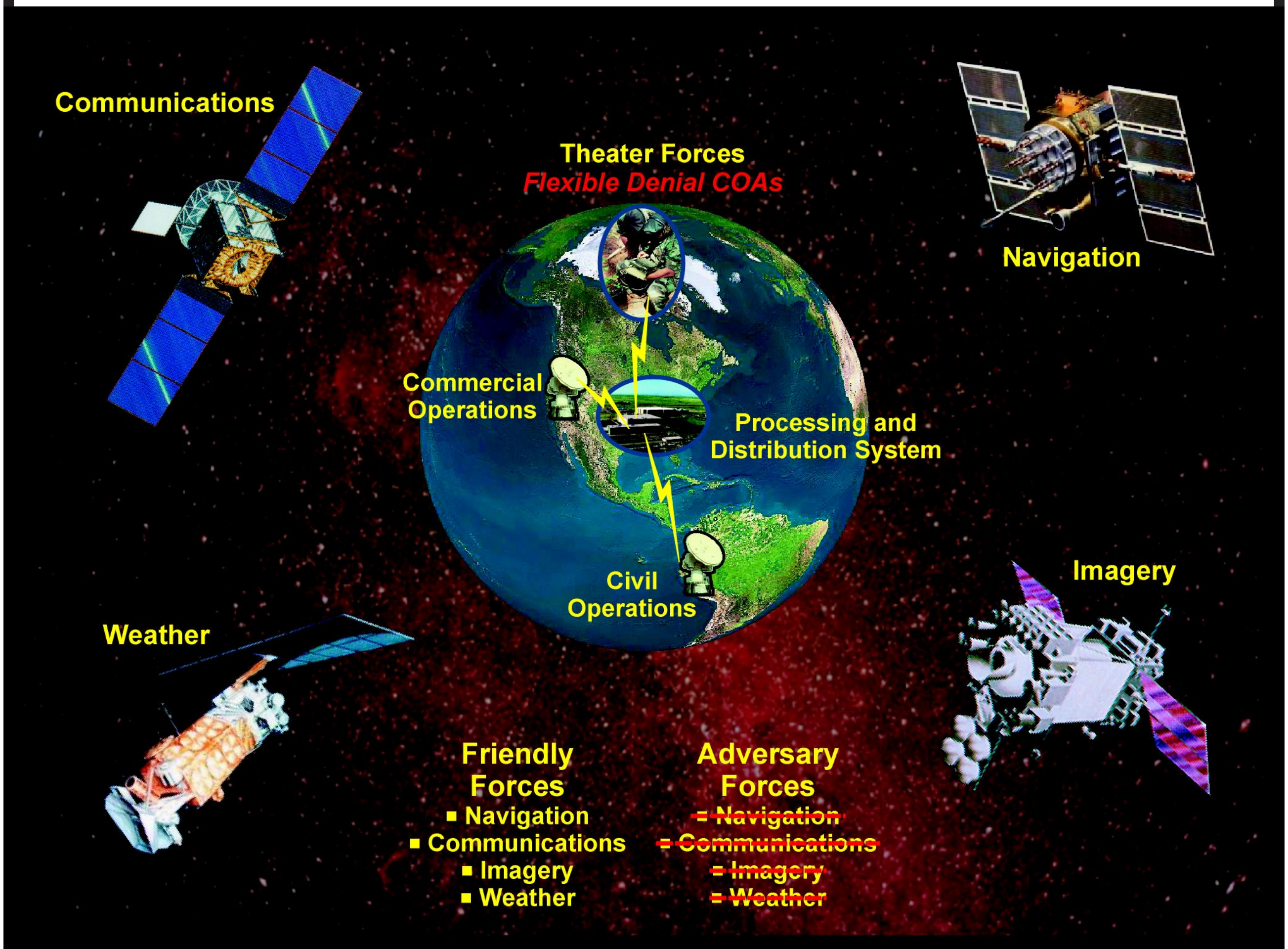
Figure 5-18 is the Prevention Roadmap, which includes candidate systems, CONOPS, organization and possible partnerships relevant to achieving the 2020 goal.

Prevention–Systems Assessment

- *Key capability–Detecting unauthorized space system use/exploitation (all systems with military utility).* No systems exist or are planned

PREVENTION

Detect Adversary's Exploitation or Unauthorized Use of US/Allied Space Systems



- *Detect Use*–Use and exploitation of US and third-party systems
- *Assess Mission Impact*–To drive course of action development
- *Timely and Flexible Reaction*–Using all actions short of military force

Figure 5-16 Key Tasks for Prevention

to satisfy this capability. Sophisticated systems for ISR can detect use, but not in a responsive way. And commercial systems will be a greater challenge whenever we know little about them. Revised ISR capabilities and CONOPS may provide partial solutions. USSPACECOM's requirements for ISR must help drive future intelligence architectures (also important to Negation). Once the information is available, N/UWSS and the USSPACECOM Battle Managers can distribute it to everyone who needs it.

- *Key capability–Assessing mission impact on US and third party systems (of national interest in minutes).* No information systems exist, or are planned for this capability. Assessment must address the US' battlespace knowledge relative to potential adversaries so we can react correctly. Advanced models and simulations will serve as a basis for course of action development. N/UWSS and the USSPACECOM Battle Managers may address part of this capability, providing all-source information and connectivity.

PREVENTION	1998	2005	2012	2020
Capabilities				
• Detect Unauthorized Space Systems Use (Blue/Gray)	10%			All System with Military Utility
• Assess Mission Impacts with High Confidence	Weeks / Days			Minutes
• Timely Flexible Denial	Days / Hours			Seconds

Figure 5-17 Prevention Capabilities and Goals for 2020

Prevention				
Key Capabilities	**Candidate Systems** 98	05	12 20	**Candidate Technologies**
Detect/ID Unauth Use/Exploit U.S. and Third Parties (100% Detect/ID all Systems with Military Utility)	N/UWSS		USSPACECOM BM	On-board Detection
Assessing Mission Impact (100% in Minutes on all National/ International Systems)	N/UWSS		GDIN	LPI, Encryption
Timely Flexible Denial (NRT, in seconds)	LPI, Encryption	CoS BM	GDIN USSPACECOM BM	On-board Software, Cross-Cueing, Encryption
CONOPS	Space AOR Space Related FDOs USSPACECOM BM	ISR for Space		
Organizations	JFSCC-Like		USSPACECOM BM	
Global Partnerships and Policies	Coalition MOA, Co-op Space Users MOA			

Figure 5-18 Prevention Roadmap

- *Key Capability–Timely flexible denial must be developed and executable (seconds).* Planned and projected systems won't fully satisfy this capability. Development of flexible denial systems, short of negation, must include features such as selective denial of GPS, low probability of intercept, and encryption. Future space system designs, operations and spacefaring nations "prevention" agreements must incorporate these factors to preclude attempts to use and exploit US and third-party space systems.

Prevention–CONOPS, Organizations, Global Partnerships and Policies

Prevention without Negation places a premium on CONOPS, organizations, and partnerships instead of hardware. A consensus approach using coalitions and diplomacy is the key to Prevention and offers solutions that systems alone can't achieve.

A collection of common systems, standards, and protocols may prevent intrusion and exploitation, if backed by innovative supporting CONOPS and organizations. A dynamic space environment offers a potential adversary many paths, but coalitions can lessen or eliminate them. Coalitions must clearly define agreements for quickly applying Prevention concepts during crises and share audits of all systems to detect and identify unauthorized use. Partnerships among the United States and other space providers, as well as between USCINCSPACE and the US intelligence community will drive progress toward rapid detection and identification of unauthorized use and exploitation. Existing organizations can support these partnerships, but new CONOPS for ISR will focus their abilities to support Prevention objectives.

In 2020, the NCA and combatant commanders will need a range of flexible options for Prevention–ranging from diplomatic, informational, and economic actions to more compelling military actions, if required.

Lastly, we believe Prevention will be enabled if space is designated an area of responsibility and if a position like a Joint Force Space Component Commander is established. We don't mean to prescribe how a regional CINC should organize space forces–only to say we must organize for space to establish Prevention leadership and responsibility and to spur progress in developing flexible options, techniques, tactics, and procedures for deterrence in space.

Prevention–Overall Assessment

We consider Prevention to be low YELLOW based on shortfalls in detecting, identifying, and reacting to unauthorized use of space systems. The growing number of, and reliance on, commercial and third-party systems pose significant challenges to preventing an adversary's use of space. But the assessment could become GREEN if major space providers cooperate on diplomatic, informational, and economic solutions (see Figure 5-19).

Prevention–Technology Assessment

Emerging technologies to address Prevention shortfalls, include an onboard ability to detect intrusion and an ability to characterize the intrusion. Encryption can help a lot, using electronic fences or keys with identification techniques common to the financial industry. Technologies that make systems tougher to intercept and can make detection and identification in near real time less critical will enhance Prevention goals.

Prevention–Recommendations and Directives

(**Recommendation**) Form an international alliance to detect and respond to unauthorized use of US and allied space systems (Department of State/ Industry/SPJ5).

(**Directive/Recommendation**) Advocate technologies, such as controlled access, encryption, and low probability of intercept, to support international Prevention (Components/Labs).

(**Directive**) Evolve doctrine so Prevention includes the range of options–non military and military–to limit an adversary's unauthorized use of space (SPJ3/J5).

(**Directive**) Develop advanced models and simulations to support analysis of Prevention nodes for operational planning and execution (N-SP/AN).

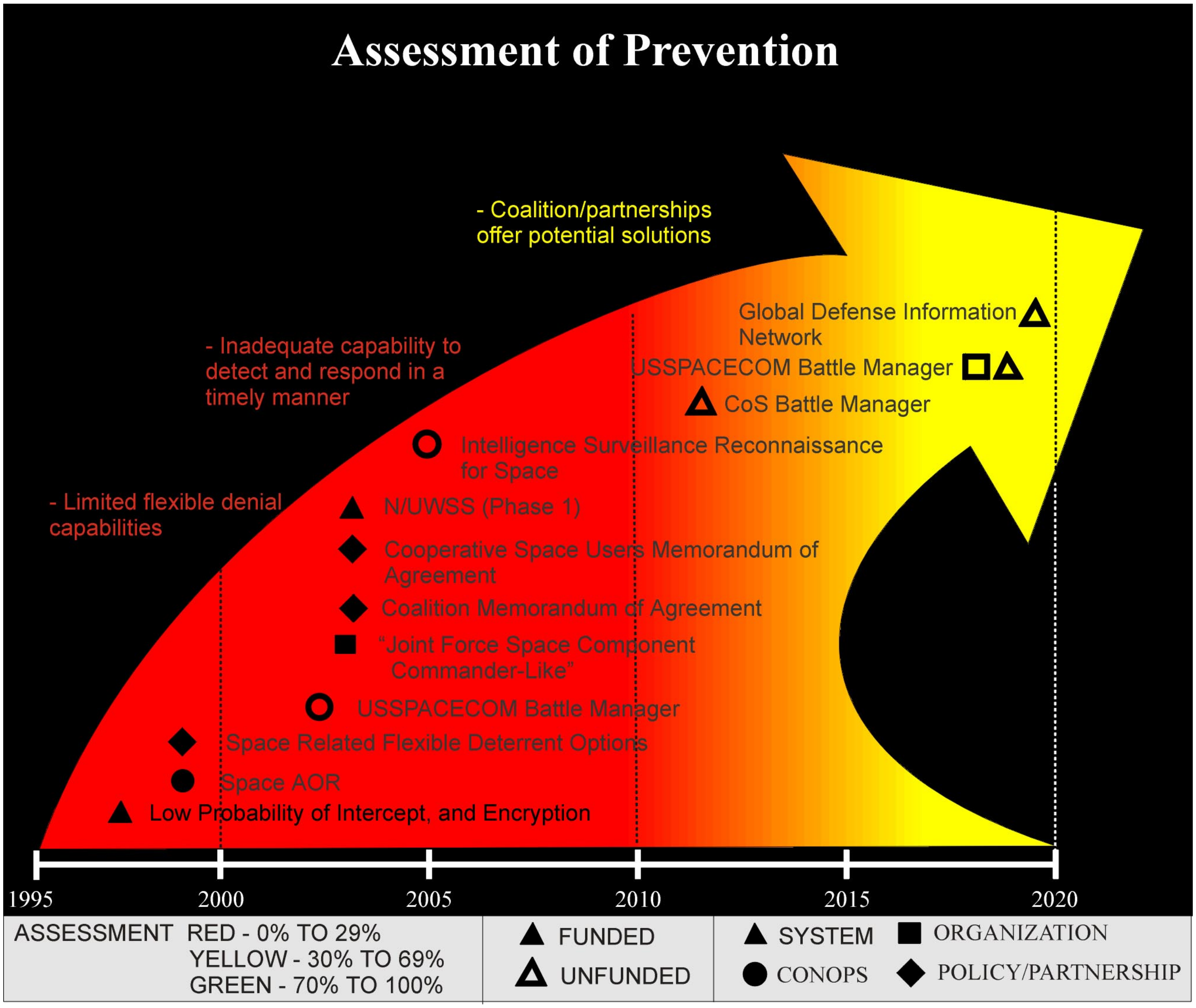


Figure 5-19 Assessment of Prevention

Negation

Negation is the ability to deny, disrupt, deceive, degrade, or destroy an adversary's space systems and services. It involves military actions to target ground-support sites and infrastructure, ground-to-space links, or spacecraft. Figure 5-20 shows key tasks for Negation.

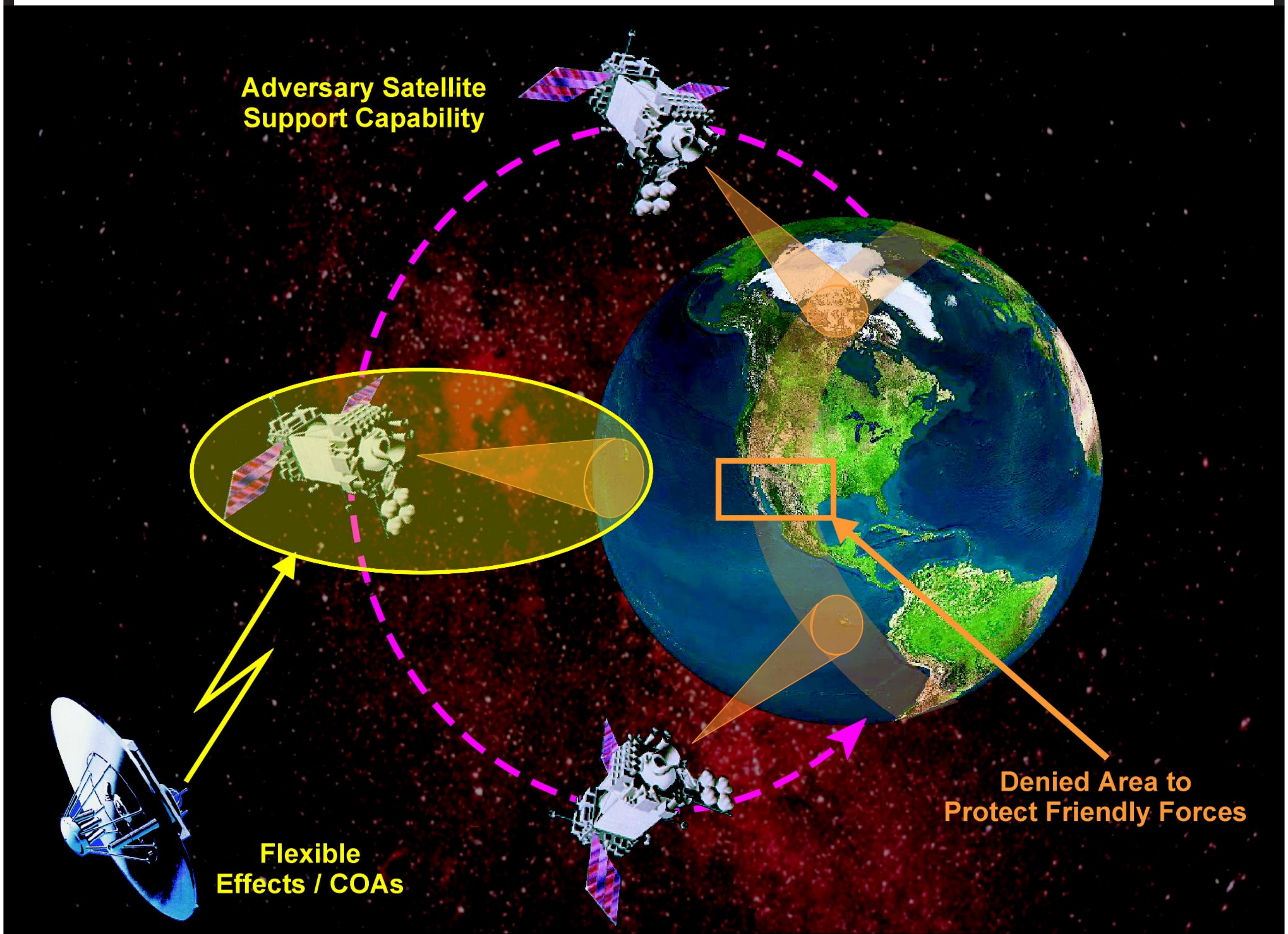
Key Capabilities for Negation

Based on the key tasks in Figure 5-20, negation requires four key capabilities in 2020.

- *Flexible effects* are required because friends and foes may use space systems at the same time. Flexible effects will achieve the range of reversible and permanent objectives for Negation–deny, disrupt, deceive, degrade, and destroy. The NCA and combatant commanders will need this flexibility to negate an enemy's systems while preserving space services for the United States and its allies.
- *Precision attack* minimizes or eliminates fratricide so we don't harm or destroy space services for United States and allies on the targeted system or near the target. As space services and products intertwine with other elements of national power, this precision becomes vital.
- *Employment on-demand* is critical because friendly forces must respond in minutes to operate faster than the adversary. To protect forces and support military operations, combatant commanders must be able to negate space systems immediately.

NEGATION

Execute Multiple/Flexible Capabilities and Effects Against Adversary Space Systems



- *Target Identification*–Complicated by a dynamic, networked environment
- *Weaponeering*–Must be precise to achieve only desired effects
- *Operations Cycle*–Includes mission planning, execution and combat assessment

Figure 5-20 Key Tasks for Negation

- *Combat assessment* allows combatant commanders to know whether negation efforts were successful. If it isn't, commanders must decide whether to strike a target again. Assessing results are very difficult whenever we're trying to negate satellites or information processing.

Figure 5-21 shows the desired warfighting capabilities, the current abilities, and the goal for 2020. Figure 5-22 is the roadmap for Negation, showing candidate systems and their enabling technologies.

NEGATION	1998	2005	2012	2020
Capabilities				
• Flexible Effects (Reversible)	5%			60%
• Precision Attack	10% GEO/LEO			100% All Nodes
• Employment On-Demand	Months / Weeks			Minutes
• Combat Assessment	Days			NRT

Figure 5-21 Negation Capabilities and Goals for 2020

Negation				
Key Capabilities	**Candidate Systems 98**	**05**	**12** / **20**	**Candidate Technologies**
Flexible Effects (60% of total capabilities must offer reversible effects)	Conventional Forces Reloc RF Jam Reloc Laser NMD GBI GBL	Small RF Kill Vehicle	SBJ SBP SOV	BIG CROW MIRACL KE ASAT HPM Tech
Precision Attack (Negate 100% of adversary space systems/services in all orbits)	Conventional Forces Reloc RF Jam Reloc Laser GBL	Small RF Kill Vehicle	SBL SBJ SBP SOV	BIG CROW MIRACL KE ASAT HPM Tech
Employ On-Demand (When required, response in minutes)	Conventional Forces Reloc RF Jam Reloc Laser GBL	Small RF Kill Vehicle	SBL SBJ SBP SOV	BIG CROW MIRACL KE ASAT HPM Tech
Combat Assessment (In NRT/100%)	TOS NMD GBI	SBEON RIDSN S-Band Fence CoS BM	SBL, SBJ, SOV, GDIN, USSPACECOM BM	Fusion Processing
CONOPS	Space AOR USSPACECOM BM	ISR For Space		
Organizations	JFSCC-Like		USSPACECOM BM	
Global Partnerships and Policies	Space Weapons Policy			

Figure 5-22 Negation Roadmap

Negation–Systems Assessment

- *Key Capability–Flexible effects–Desired mix of permanent (40%) and temporary (60%) effects.* Programmed and planned systems will meet the requirement for flexible effects. The US' evolving ability to launch a conventional attack on ground stations and supporting infrastructure, as well as the Ground-Based Interceptor for National Missile Defense, satisfy requirements for permanent effects. Planned systems, including relocatable radio-frequency and laser jammers, Ground-Based Lasers, Space-Based Jammers, and the Space Operations Vehicle cover temporary or non-lethal actions. The Space-Based Jammers and Space-Based Lasers appear to be the most versatile in providing options for temporary effects on anticipated targets. Information operations, though not addressed, may do this more efficiently. Planned systems and information operations rely heavily on high volumes of precise information from sensors to shooters, who must have it in near real time. If they don't get precise information quickly, lasers or information operations could destroy systems.

- *Key Capability–Precision attack against an adversary's space system (limited target set, 100% of the time, all nodes).* Programmed and planned systems will attack precisely. Present systems include conventional attack against ground sites and supporting infrastructure, but planned systems will greatly improve this ability by 2020. Radio frequency and laser systems–fixed and mobile–will attack precisely against targets near Earth.

  Emerging space and telecommunications trends that tailor services to specific regions or users will complicate engagements for Negation forces because information flows seamlessly across a global infrastructure. We must solve this problem with better equipment and procedures. Questions emerge: Should we "fix" systems or make them mobile? Do we have enough systems with access to targets? Can we solve support issues, such as basing rights or deployment logistics? The Space-Based Jammer and Laser don't have these problems. Just as information operations can cause flexible effects, they can also attack precisely. But, in all cases, sensors will need to provide shooters with a lot of precise technical and operational intelligence.

- *Key Capability–Employment On-Demand against all nodes of an adversary's space system (limited target set), whenever required (minutes).* Planned systems will satisfy requirements for employment on demand. Today, conventional forces can't respond quickly enough because of problems with support in far-flung operating locations. Likewise, applications using National Missile Defense Ground-Based Interceptor depend on line-of-sight. Some planned systems, such as the Ground-Based Laser and relocatable platforms using radio frequencies or lasers, have the same shortfalls. Abilities envisioned for the Radar Imaging Deep Space Network, as well as Space-Based Radars, Lasers, and Platforms, will meet goals for on-demand employment. Constellations must be robust enough to place "eyes" completely on the targets.

- *Key Capability–Combat assessment against limited target set (near real time).* Planned and programmed systems do not fully address demanding requirements for assessing results of flexible effects and precision attack. Today, Ground-Based Lasers, optics, and radars can see only the gross physical characteristics of lethal attacks. Information operations and ISR assets permit fairly comprehensive combat assessment. But, these systems support a range of national and theater customers who would likely preempt them for other missions. For that reason, planned negation systems must either include their own equipment to assess results or get the information from other intelligence-gathering systems. The Space-Based Electro-Optical Network, Radar, and Laser offer high resolution imagery without atmospheric distortions that affect ground-based systems. Though not addressed, information operations–such as attacks on computers–can also assess results when an action doesn't cause observable damage. Infrared sensors, especially space-based ones, can assess results when physical damage is limited. Planned systems must address new approaches to ISR, employing active collection approaches associated with information operations.

Negation–CONOPS, Organizations, Global Partnerships and Policies

Integrating complex, overlapping Negation operations with the regional CINC's campaign plan will require CONOPS for space superiority (single operational focus); force protection (counter antisatellite); and Prevention and Negation. Designating space as an area of responsibility will enable USCINCSPACE to develop, plan, coordinate, and execute combat operations in space.

A Joint Force Space Component Commander-like position will integrate space operations with theater planning to coordinate Negation requirements. Also, the USSPACECOM Battle Managers will support this organization by managing information and tasking in near real time.

As on-orbit systems and space debris increase, many more objects reenter the Earth's atmosphere. In fact, because spacecraft use composite materials, they will often reenter intact. We'll need to partner with other players in space to reduce the dangers of these reentries.

The United States will need to develop national policies supporting space warfare, weapons development and employment, and rules of engagement. Key allies, theater commanders, and agencies will have to coordinate on these policies.

Negation–Overall Assessment

Our overall assessment for Negation is YELLOW because planned and programmed systems satisfy all Negation capabilities except combat assessment (see Figure 5-23).

Negation–Technology Assessment

Today, we have conventional abilities that produce mostly permanent effects against satellite ground stations. In the future, we need land, sea, air and space-based systems. These flexible, negation systems must strike precisely to produce reversible and permanent effects against all nodes of a potential adversary's space systems. They must act in near real time and not harm systems belonging to allies or neutral players.

Laser and radio frequency technologies offer promise to provide improved permanent effects without fratricide to friendly and neutral systems. We need to develop devices using chemical oxygen-iodine lasers (COIL), free-electron lasers, nonlinear optics, passive and active high-resolution imaging, beam control, optical sensing technologies, and high-power optical components, and ways of establishing the vulnerability of a target.

High-Power Microwaves may be able to disrupt, degrade, and destroy electronics in communication and information systems. They would use bandwidths at high peak power to damage electronic information processing and communications or bandwidths at high average power to disrupt them. Efforts are underway on radio-frequency sources and effects, antennas, and pulsed-power systems. Digital radio-frequency memory can accurately store, replicate, and manipulate coherent signals for retransmission, thus degrading a threatening sensor's ability. Microwave power modules also are much smaller and more efficient than typical transmitters using vacuum tubes or transistors.

In addition to ground-, air-, and space-based lasers, radio-frequency transmitters, and microwave technologies, the military Space Operations Vehicle and space-based weapons would give the United States enough flexibility to meet future Negation requirements. The military Space Operations Vehicle and Space-Based Lasers are inherently flexible because they offer options for reversible and non-lethal effects. But the Space Operations Vehicle will require lightweight, durable thermal protection and revolutionary propulsion systems, as well as other technologies outlined under Assured Access.

The military Space Operations Vehicle and space-based weapons can perform temporary and permanent jamming, strike satellites, and blind space sensors. Ground-Based Lasers are being developed and demonstrated to support antisatellite systems. A central part of the effort is the Air Force's demonstration of integrated beam control with parallel development for the COIL device, high-power optical components, and assessments of a satellite's vulnerability. Jamming will require laser sources to provide the precisely directed, highly intense beams of coherent, mid-infrared, jamming energy.

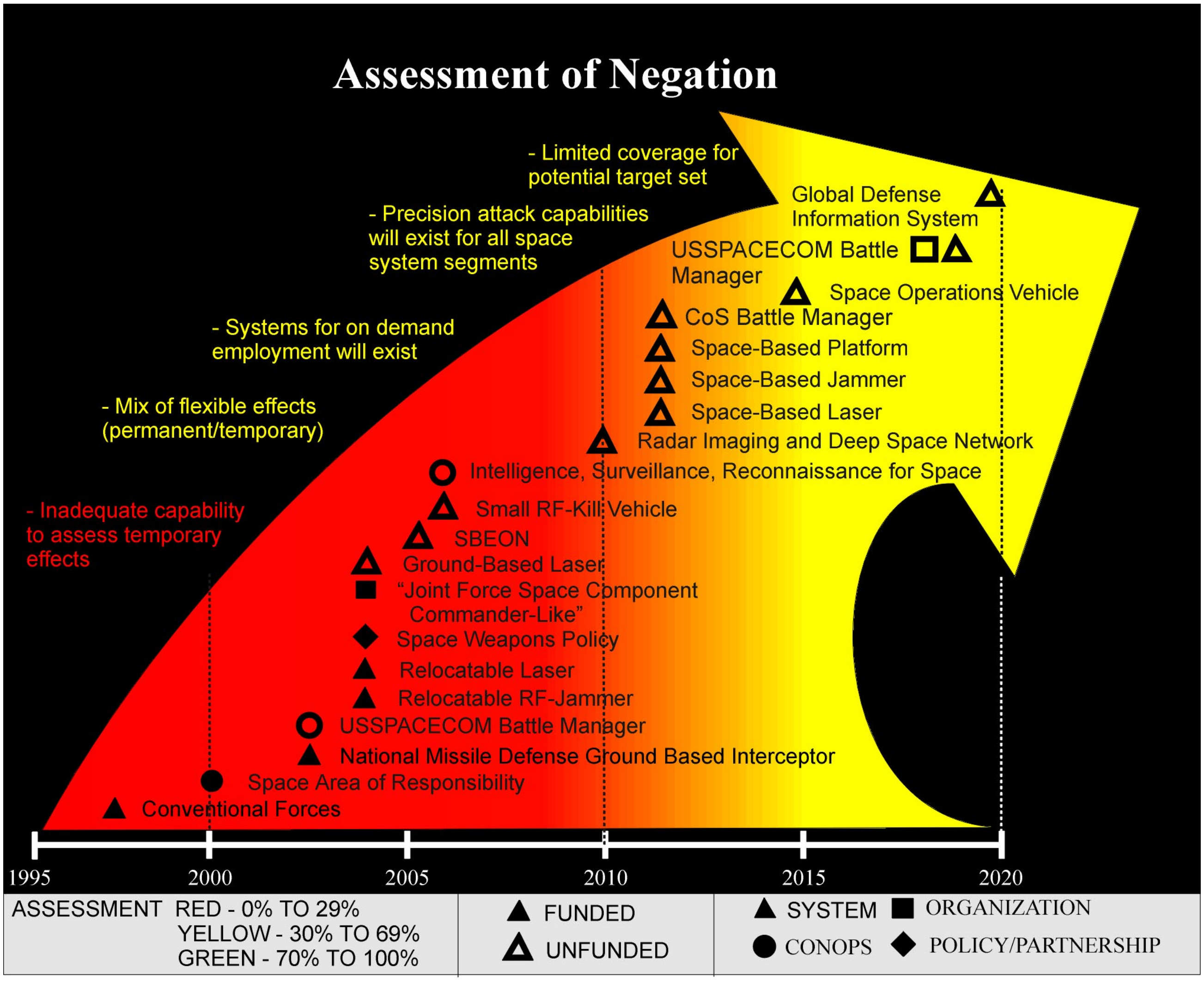


Figure 5-23 Assessment for Negation

Semi-conductor laser diodes are very efficient, bright, lightweight, and compact. Technologies for information operations may also be able to temporarily deny, disrupt, and degrade enemy systems.

By 2020, when USCINCSPACE becomes a supported commander, battle-management technologies must mature to create a seamless net serving USCINCSPACE, other combatant CINCs, and combat-support agencies for execution in hours or even minutes. Battle management must include assessing the success of Negation missions. This assessment will be toughest for temporary effects.

Negation–Recommendations and Directives

(**Directive**) Advocate programs for flexible, precision attack via land, air, sea, and space (SPJ3).

(**Directive**) Advocate the ability to assess Negation results onboard, as a complement to national or theater systems (SPJ3).

(**Recommendation**) Advocate national policy and legislation to support Negation (SPJ5).

(**Directive**) Evolve doctrine to consolidate Negation with Prevention (SPJ5).

SUMMARY ASSESSMENT

The overall assessment is YELLOW based on combining the ratings of the five specified objectives:

- *Assured Access* is GREEN in 2020, if required systems, CONOPS partnerships, and policies are available.
- *Surveillance of Space* is YELLOW in 2020 if we can credibly analyze the space surveillance system's performance. A GREEN rating requires strong advances in quickly characterizing space objects, as well as improvements in locating and sizing orbits.
- *Protection* in 2020 is low YELLOW. To achieve a YELLOW rating, we must develop and incorporate emerging technologies for affordable, lightweight, and effective systems that detect threats.
- *Prevention* in 2020 is rated a low YELLOW, with large shortfalls. Systems, CONOPS, and organizations must be planned and developed to address the deficiencies. But partnering efforts could increase the rating to GREEN.
- *Negation* is YELLOW, despite the range of negation equipment projected for 2020, because it won't have systems to assess its success.

Prioritized Capabilities

We developed critical capabilities by focusing on those which (1) support multiple objectives, (2) address a near-term threat, and (3) enable other capabilities by providing resources or because they must exist before we can carry out the others. For example, characterizing high-interest objects in real time is a primary surveillance capability that supports the ability to protect our space systems and negate an adversary's. In addition, the growing number of satellite services being developed and deployed by organizations outside the United States means characterizing these objects is a near-term threat. Finally, characterizing high interest objects logically precedes the ability to target, attack, and assess effects.

As you read the following lists, keep in mind that we consider all key capabilities important but must identify critical ones due to constrained resources.

Critical capabilities are essential to gain freedom of operations in space and denying that freedom to others. So we gave priority to capabilities that preserve our space advantage and improve our situational understanding of space, including knowledge about US and allied systems, potential threats, and unauthorized use. It's also essential to be able to change the space force structure, so we can counter or gain an advantage over an adversary.

Critical Capabilities

Real Time Characterization of High Interest Objects (Surveillance of Space)
Detect & Report Threat/Attack (Protection)
Detect Unauthorized Space Systems Use and Exploitation (Prevention)
Recoverable Rapid Transport to/through/from Space (Assured Access)
Modeling & Simulation (All)
Flexible Effects (Negation)
USSPACECOM Battle Managers (All)
Global Traffic Control (Assured Access)

Key Capabilities

Assess Mission Impact (Protection/Prevention)
Combat Assessment (Negation)
Timely Surveillance of High Interest Objects (Surveillance of Space)
On-Demand Satellite Deployment (Assured Access)
Launch to Sustain Required Constellations for Peacetime (Assured Access)
Precision Attack (Negation)
Employment on Demand (Negation)
Detect/Track Precise Size & Location (Surveillance of Space)
ID/Locate/Classify Source (Surveillance of Space)
Timely Flexible Denial (Prevention)
Withstand & Defend (Protection)
Catalog/Monitoring (Protection)
Reconstitute & Repair (Protection)
On-Demand SATOPS Execution (Assured Access)
Integrated SATOPS Mission Planning (Assured Access)